

B.C. Ministry of Health Data Governance Framework Overview

July 31, 2013
DRAFT for discussion



Contents

- Definition & guiding principles
- Data governance framework
- Supporting processes
- Appendix - Detailed role descriptions
 - Data Governance Lead
 - Data Officers

Definition & guiding principles

“Data Governance” defined

Why is Data Governance important?

- When implemented correctly across the Ministry, data governance will have the following benefits:
 - Clarification around accountability, roles and responsibilities for data
 - Improved decision making framework that ensures that decisions are made at the right level in a prioritized and risk-based manner
 - Improved efficiency and productivity through standard and repeatable business processes
 - Enable achievement strategic and operational objectives through timely access to data
 - Reduce risk by ensuring data is adequately and consistently protected

Ministry definition:

“Data governance” is the framework that promotes roles, responsibilities, processes, standards and policies to ensure the consistent and transparent management, maintenance, and utilization of Ministry data while mitigating risk.

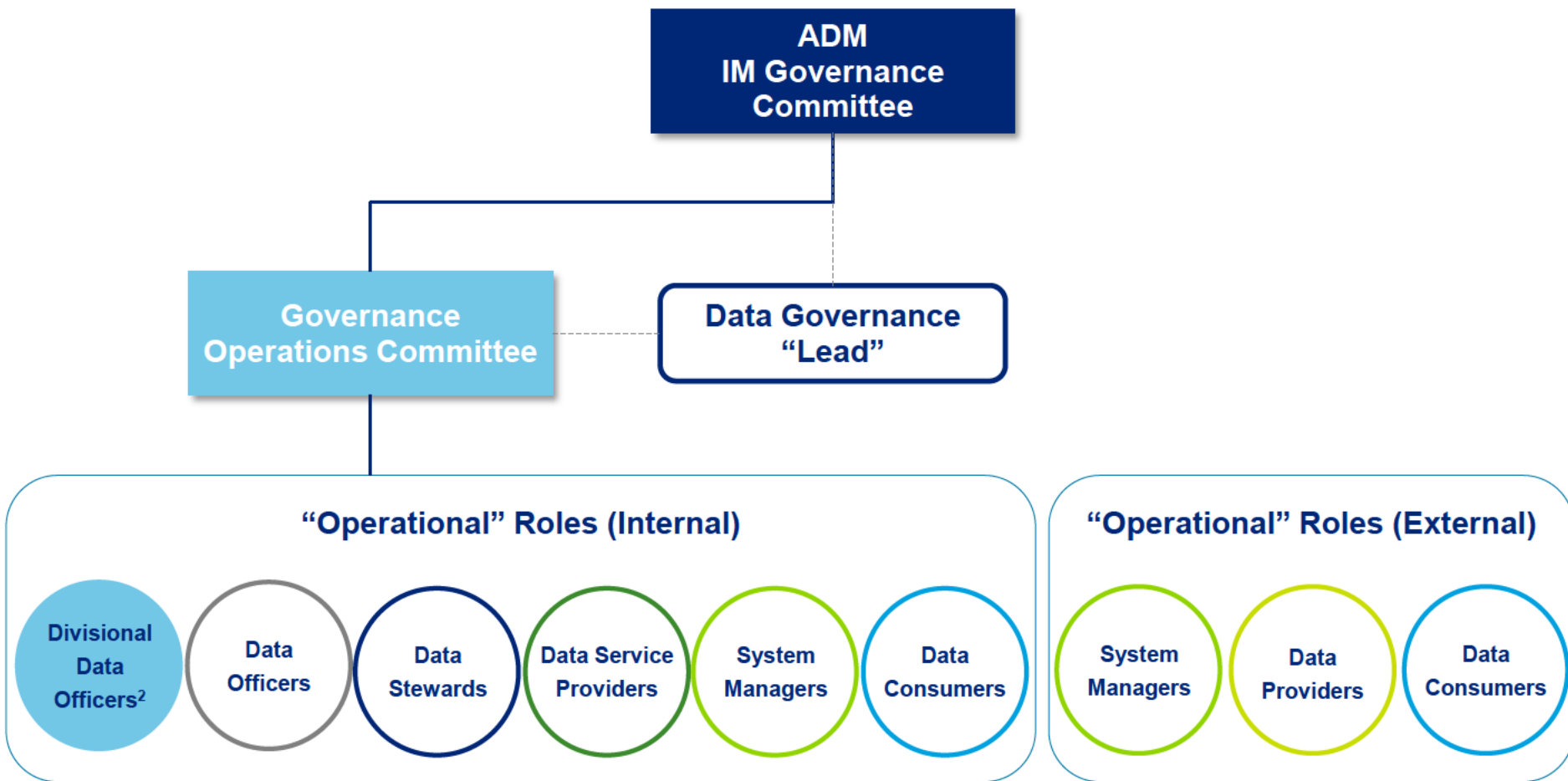
Data governance “principles”

The Data Governance principles listed below establish the objectives for the Ministry’s Data Governance Framework and will serve to guide decisions and requirements established to operationalize the framework:

Principle 1	The Ministry values and respects data as an asset
Principle 2	Individuals understand their accountabilities for data
Principle 3	The Ministry collects, uses and discloses data for purposes consistent with its mandate and as authorized under applicable legislation
Principle 4	Authorized users can access data in support of the operational and strategic objectives of the Ministry
Principle 5	Decisions concerning data use and disclosure are made and prioritized at the appropriate level based on a transparent, consistent and risk-based decision-making process
Principle 6	The Ministry uses and discloses data in the least identifiable format possible to accomplish the intended purpose
Principle 7	The Ministry creates an adaptive, transparent and collaborative environment to support effective information management.
Principle 8	Data quality and consistent processes support timely and effective decision making and reporting

Data governance framework

Ministry's Governance model¹

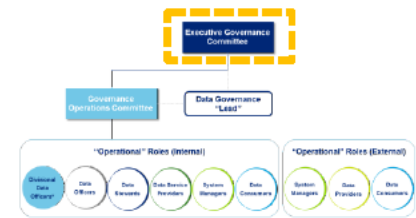


¹ See Data Governance Handbook document for additional details regarding Committees and roles defined in this presentation.

² Governance Operations Committee will be composed of Data Officers

IM Governance Committee

Purpose



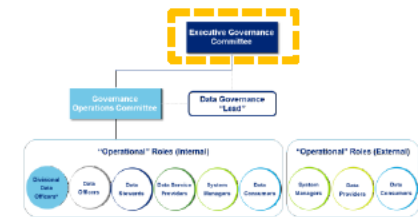
- The IM Governance Committee is a senior team of Ministry representatives responsible for overseeing, endorsing and deciding on various aspects of data governance
- The IM Governance Committee is accountable for operationalizing the Ministry's data governance principles through the following activities:
 - Defining the **strategy for data governance**
 - **Prioritization and resource allocation for initiatives** related to data management
 - **Endorsement of data management policies** (including those related to data terminology, quality, protection, technology and management)
 - **Ensuring compliance mechanisms are in place** to monitor and verify adherence to data management policies and regulatory requirements

“Information management” refers to the collection, use, disclosure, retention, destruction, protection, quality and availability of Ministry data.

IM Governance Committee

Scope and responsibilities

- The IM Governance Committee has overall responsibility and accountability for Ministry data
- Its objective is to provide oversight and set direction on roles, responsibilities, processes, standards and policies as well as ensure consistent and transparent management, maintenance and utilization of Ministry data while mitigating risk
- The extent to which the IMGc's mandate will include analytics will be determined following completion of the analytics strategy
- Areas of specific focus under this mandate include:

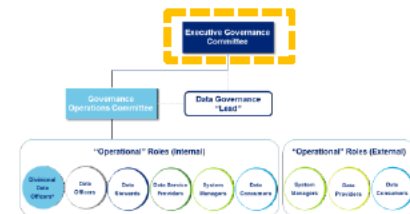


The IM Governance Committee:

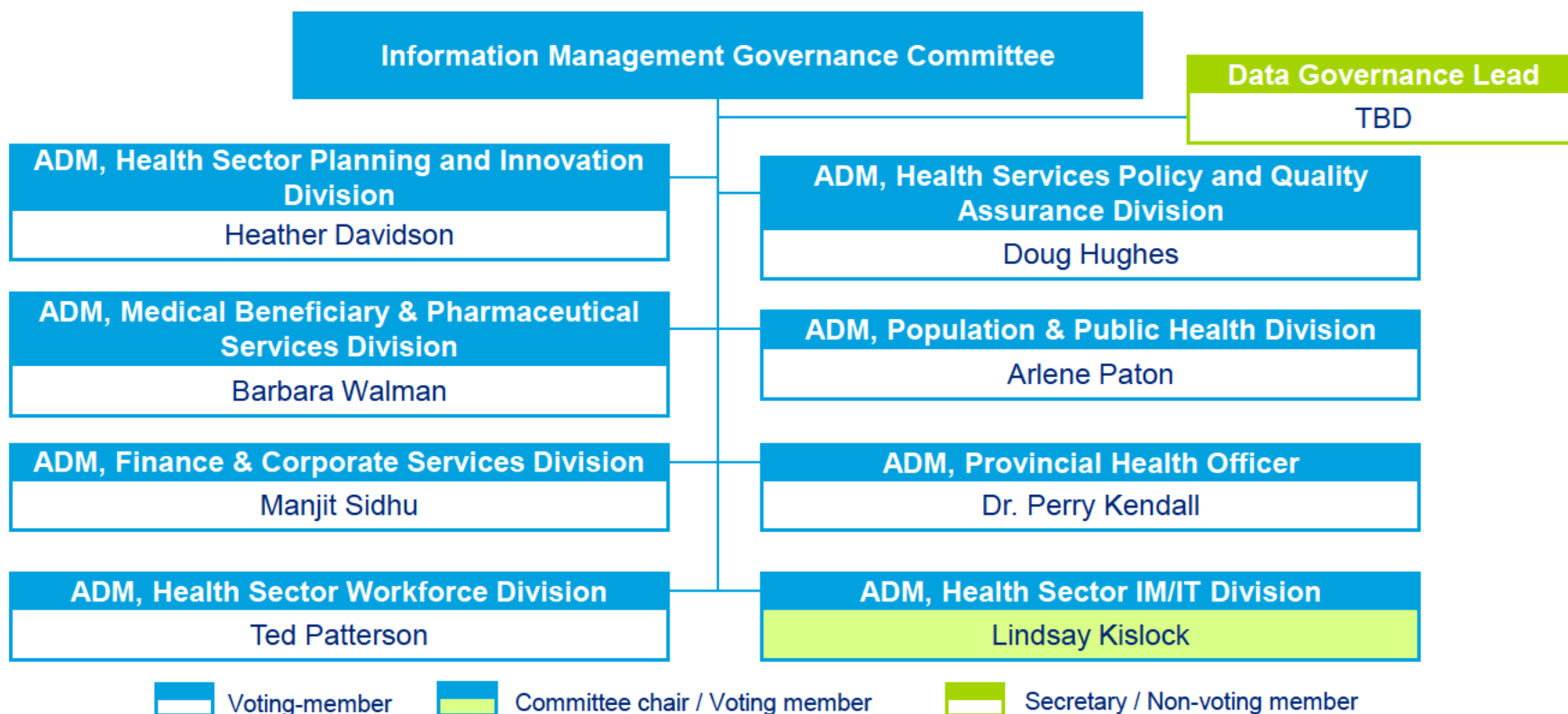
- ✓ Responsible for setting Ministry direction and strategy in relation to IM and data governance, including the provision of strategic direction in relation to utilizing Ministry data as a corporate asset (with respect to risk mitigation and business enablement)
- ✓ Defines data governance strategic priorities
- ✓ Establishes, endorses and reviews the Ministry's data governance policies and standards
- ✓ Is accountable for the Ministry's overall compliance with IM policy and legislation
- ✓ Manages and approves the Ministry's investment in data assets that impact multiple Divisions
- ✓ Allocates Data Officer resources to the Governance Operations (GO) Committee and to data-related initiatives on a priority basis
- ✓ Provides direction to GO Committee and Data Officers, as required
- ✓ Serves as the final decision-making body for escalated data governance issues and decisions
- ✓ Establishes KPIs for measuring and reporting on the management of and compliance with the Data Governance Framework

IM Governance Committee

Membership



- The Committee is comprised of the most senior representatives of the Business and IM functions (ADMs) with authority to act on behalf of their respective divisions
- The Data Governance Lead will serve as the secretary for the Committee as well as participate in the Committee as a non-voting member



IM Governance Committee

Supporting structures



Data Governance Lead

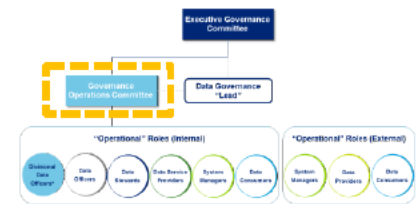
- Data Governance Lead will be appointed by and accountable to the Health Sector IM/IT (HSIMT) ADM
- The Data Governance lead will be the **single person accountable for the implementation and operation of data governance**
- The Data Governance Lead will **support decision making within the IM Governance Committee and GO Committee**, as well as the execution of their respective mandates
- The scope of Data Governance Lead's responsibilities may be amended from time to time by the IMGCC
- See Appendix – Data Governance Lead Job Description

The scope of responsibilities of the Data Governance Lead includes:

- ✓ Supporting the effective implementation of the Data Governance Framework;
- ✓ Supporting the development of governance policy, standards and processes and ensuring alignment with corporate and/or government policies, standards and processes;
- ✓ Managing all aspects of day-to-day data governance activities including communications, measurement and reporting;
- ✓ Reviewing and advising on Executive decisions for data governance initiatives;
- ✓ Managing the GO Committee project portfolio,
- ✓ Supporting operational reporting on data governance metrics.

IM Governance Committee

Supporting structures (cont.)

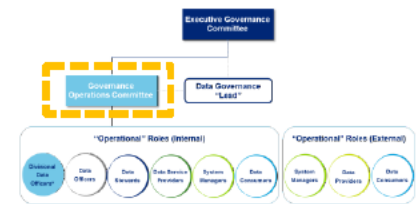


Governance Operations (GO) Committee

- Members of the IM Governance Committee are responsible for identifying a senior level staff member to serve as their Data Officer
- Data Officers will be accountable for their Division's interactions with data; including, data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction)
- Data Officers will represent the Division's interests in relation to data management and governance and serve as the accountable party for ensuring that data governance requirements, including principles, policies and standards, are operationalized within their Division (see Appendix – Data Officer Job Description)
- Although the Data Officer would have overall accountability for data governance within a Division, s/he may delegate data governance activities to other team members, referred to as Data Officers, as needed
- Data Officers will collaborate through the Governance Operations (GO) Committee
- The IM Governance Committee will assign tasks to a Data Officer(s) through the GO Committee, in order to operationalize the Data Governance Framework and address governance-related priorities

IM Governance Committee

Supporting structures (cont.)



Governance Operations (GO) Committee

The IMG Committee can delegate the following types of data-related decisions and activities to the GO Committee:

- ✓ Representing the data interests of respective Divisions in the delivery of the Ministry's strategic and operational objectives
- ✓ Defining, prioritizing and operationalizing a portfolio of data-related projects that address strategic priorities set by the IMG Committee
- ✓ Raising and resolving key operational data issues and decisions in relation to data terminology, quality, protection, technology and management
- ✓ Providing recommendations to the IMG Committee on responsibilities, processes, standards and policies in relation to Ministry data as well as key data governance issues, risks and decisions;
- ✓ Providing periodic reporting on the project portfolio
- ✓ Escalating risks/decisions to the IMG Committee
- ✓ Supporting IMG Committee decision-making on escalated issues by preparing decision support material and presenting to the Committee as required
- ✓ Periodic reporting to the IMG Committee that addresses data-related KPIs (i.e. quality, training, project progress, DSAs, etc.)

IM Governance Committee

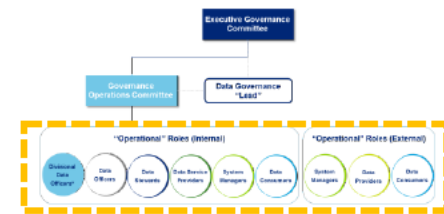
Supporting structures (cont.)

Additional Committee Members

- Additional representation may be included within the IMG and GO Committees as required
- Specifically, additional subject matter expertise may be required in certain disciplines, such as privacy (through the Chief Privacy Officer or delegate), information security, analytics, research, vital statistics or other subject areas
- These members may be appointed to both the IMG Committee and the GO Committee on an ad-hoc or permanent basis as agreed to by all members of the respective committees.

Ministry's Governance model

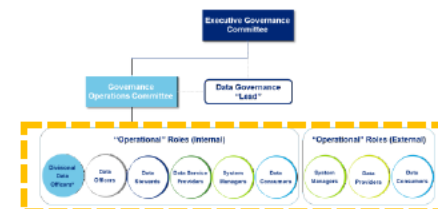
Operational roles






- Data governance operational roles allow for the identification of data governance related responsibilities by types of roles that exist across the information lifecycle (**Note:** individuals may have multiple data governance roles that they function in at any point in time)
- The following slides provide a high-level overview of the Ministry's data governance operational roles (see Data Governance Handbook for additional details)

Ministry's Governance model

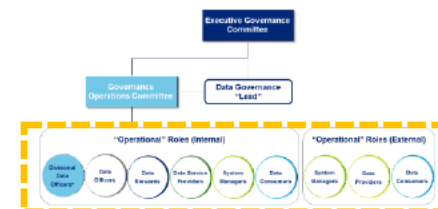
Operational roles






Role	Description	Guidance
	Each Division will appoint a Data Officer. Data Officers are responsible for the management and oversight of data handling and management within an individual division (See job description in Appendix). Data Officer will represent the Division on the GO Committee.	<ul style="list-style-type: none"> IM Governance Terms of Reference Policy Job Description
	Data Stewards are accountable for the management of data repositories or data products. Examples include databases, linked datasets, reports and repositories (e.g., LAN folders). Data Steward responsibilities include access management (i.e. requests/reviews for individual systems/repositories) and ensuring compliance of data set controls with applicable policies (i.e. data security, Information Sharing Agreements, privilege management, etc.). Data Steward responsibilities may be limited to an individual file or extract, which will reduce or eliminate administrative stewardship requirements, and result in only a requirement to protect data in compliance with applicable requirements.	<ul style="list-style-type: none"> Policy Legislation Job Description
	Data Service Providers are individuals who receive requests for data and related analysis and data processing activities (e.g., dataset linkage). These requests can be received from internal or external stakeholders and require Data Service Providers to extract information (from a system or from multiple systems and/or datasets), manipulate it, prepare it and distribute it to the requestor (Data Consumer). They are required to know their responsibilities with respect to providing data in compliance with the Ministry's policies and standards as well as the Ministry's legislative and contractual obligations	<ul style="list-style-type: none"> Policy Legislation Job Description

Ministry's Governance model

Operational roles



Role	Description	Guidance
 <p>System Managers</p>	<p>System managers manage the Ministry's systems and infrastructure. System managers are responsible for the maintenance of IT infrastructure in compliance with Ministry policy on behalf of one or more division. Examples would include HSIMIT and Maximus.</p>	<ul style="list-style-type: none"> • SLAs • Contracts, ISA • Policy (internal) • Legislation
 <p>Data Consumers</p>	<p>Data Consumers are the end users of data and can be either internal or external to the Ministry. Data consumers are responsible for adhering to applicable Ministry data policies and processes. Data consumers are categorized into 3 areas depending on their level of data interaction:</p> <ul style="list-style-type: none"> • Highly facilitated – individuals consume reports, dashboards and other “prepackaged” data • Moderately facilitated – Individuals can generate reports and content based on structured and often predefined report parameters • Raw data – Individuals can directly interact with data and manipulate it, link it and otherwise create value through it in a variety of ways (e.g. economic modeling, analytics, etc.) 	<ul style="list-style-type: none"> • Policy (internal) • Legislation • Contract, ISA
 <p>Data Providers</p>	<p>Health care providers and organizations who provide data to the Ministry (e.g. doctors, Health Authorities, CIHI, etc.)</p>	<ul style="list-style-type: none"> • Contracts, ISA • Legislation

IM Governance Committee Terms of Reference

- The Information Management (IM) Governance Committee Terms of Reference (TOR) serves as the basis for the DG Framework and provides additional detail regarding the roles and committees described above
- It incorporates components of the former IMGC Terms of Reference, Data Stewardship Terms of Reference and other leading practices for Data Governance Terms of Reference
- Endorsement of the IM Governance Committee TOR serves as the formal basis for the Data Governance Framework, empowering the Governance Operations Committee to start its work, and create the Data Governance Lead role

IM Governance Committee TOR addresses the following:

- | | |
|--|---|
| — Purpose | — Decision making protocols (i.e. Quorum, Voting and Escalation triggers) |
| — Scope and responsibilities | — Meeting logistics |
| — Membership (unchanged) | — Deliverables and supporting documentation |
| — Supporting structures (including the Data Governance Lead and Governance Operations Committee) | — Reporting protocol |

Supporting processes

Supporting data governance processes

Issues assessment process

- The purpose of this process is to provide a mechanism for data-related issues to be:
 - Identified
 - consistently documented
 - assessed
 - resolved or escalated as required
- Three key steps:
 - **Identification** - issues can be identified and raised by anyone (end user, business owner, IT representative, etc.). They should be reported to the Data Officer for evaluation and potential resolution.
 - **Assessment** – if the issue cannot be resolved, the DO will document the issue in an issue log and escalate to the office of the Data Governance Lead
 - **Resolution** - once assessed and documented, the issue will be raised to the Governance Operations Committee for resolution. If resolution is not possible, the issue is escalated to the IM Governance Committee as needed

Issue Assessment Process

Identification

- Identify issue
- Preliminary assessment
- Close/escalate

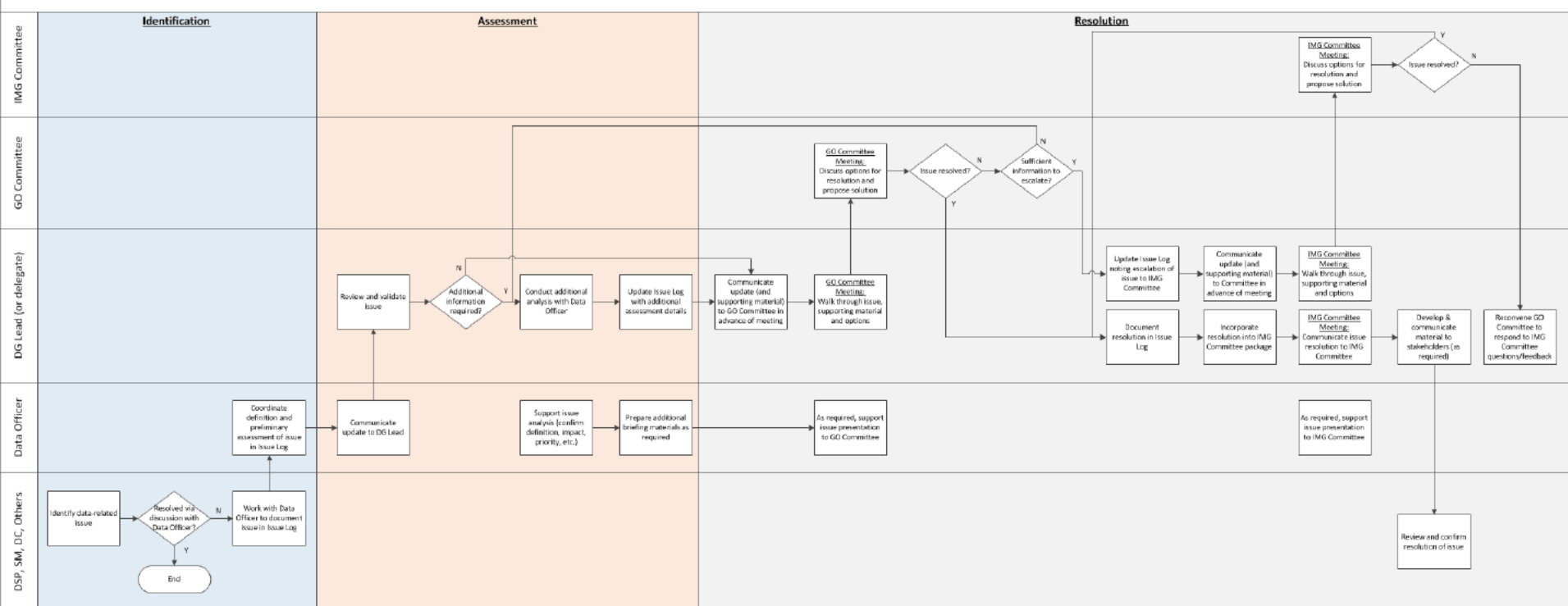
Assessment

- Gather additional information
- Update issue log
- Prepare presentation

Resolution

- Present
- Resolve/escalate
- Close & communicate

Issue Assessment & Resolution Process



Appendix

Data Governance Lead Job Description

Roles & Responsibilities

- Responsible for managing all aspects of the day-to-day data governance activities including communications, measurement and reporting
- Serves as the secretary to the Executive Committee and Governance Operations Committee and supports their operation (Note: over time this role can range from a secretariat/support function for existing decision-making bodies to a formal data governance authority with additional areas of responsibility)
- Proactively represents corporate governance in relation to the following:
 - Supporting the effective implementation of the Data Governance Framework
 - Supporting the development of governance policy, standards and processes
 - Reviewing and advising on Executive decisions for data governance initiatives
 - Supporting operational reporting on data governance metrics and KPIs
- Communication of data governance decisions across the Ministry to the Executive as well as Data Stewards, as appropriate.

Skills and Knowledge

- Necessary business experience to understand how data can be utilized within the Ministry, along with the ability to communicate with Executive and Data Stewards to understand their data and information needs; provide guidance and direction on usage of Ministry data; and develop measurements and reporting for Executive.
- Problem solving complex data interactions including risk and value impact analysis and prioritization.

Measurements

- Attendance and participation in Governance Operations Committee and Executive Committee meetings as reflected in the minutes and communications.
- On time completion of Governance Operations Committee's data governance portfolio projects.
- Number of data issues for their division that have been analyzed and resolved.
- Satisfaction of committee members being represented measured through quarterly survey and data community testimonials.
- Data governance score card with defined performance metrics.

Data Officer Job Description

Roles & Responsibilities

- Responsible for the Divisions interactions with data, including data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction).
- Proactively represents their Division in relation to the following:
 - Appropriate use of the data within the division
 - The escalation point for reporting and resolving data issues
 - Cross Ministry liaisons with other members of the GO Committee to review and assess common/shared data issues
 - Manage and be accountable for enterprise and division-specific data governance project portfolio
 - Recommend actions to be taken to resolve data issues
 - As required, inform or be a direct participant in work packages / projects with respect to data domains
 - Develop implementation plans for data within their division to address priorities set by IM Governance Committee
 - Report on progress against action plans
- Communication of data governance decisions out to their Divisions, as appropriate.

Skills and Knowledge

- Problem solving complex data interactions including risk and value impact analysis and prioritization.
- Ability to liaise with technical staff and translate technological data circumstance to business terms.
- Good understanding of data lifecycle and usage within their division, including processes for data origination, processing and controls.

Measurements

- Attendance and participation in GO Team meetings as reflected in the minutes and communications.
- On time completion of data governance portfolio projects
- Number of data issues for their division that have been analyzed and resolved.
- Satisfaction of division stakeholders being represented measured through quarterly survey and data community testimonials.
- Data governance score card with defined performance metrics for the division.

Deloitte.

Ministry of Health

Data Governance Handbook

Owner Data Governance Lead

Version Final Draft for Discussion 0.4

Change Record

Version	Date	Description of Changes
0.1	July 13, 2013	First draft completed.
0.2	July 20, 2013	Edits based on team feedback.
0.3	July 31, 2013	Updated based on edits to IMG Committee TOR and related feedback
0.4	August 5, 2013	Updated based on additional feedback received.
Final:		

Contents

Contents

Contents	3
1 Introduction	4
1.1 Purpose	4
1.2 Audience	4
1.3 Scope.....	4
2 Data governance defined.....	5
3 Data governance framework overview	6
3.1 Governance model overview.....	6
3.2 Executive Governance Committee	7
3.3 Supporting roles and structures	7
3.4 Operational data governance roles.....	8
4 Supporting processes	12
4.1 Issues Assessment Process	12
5 Deployment.....	14
6 Data governance glossary	15
Appendix A: Information Management Governance Committee Terms of Reference.....	17

1 Introduction

The Ministry of Health (“MOH” or “the Ministry”) Data Governance Framework is designed to enable and support the Ministry in the delivery of its mandate through the effective management of information and information technologies, in order to meet the four primary goals of the Ministry’s Service Plan¹:

1. Improved health and wellness for British Columbians.
2. British Columbians have the majority of their health needs met by high quality community based health care and support services.
3. British Columbians have access to high quality acute care services when they need them.
4. Improved innovation, productivity and efficiency in the delivery of health services.

1.1 Purpose

The purpose of the Data Governance Handbook is to provide a reference for the Ministry and its Information Management Governance (IMG) Committee on the data governance program. It provides an overview of the Ministry’s Data Governance Framework including definitions, guiding principles, key roles and responsibilities and supporting structures as well as a roadmap which outlines key next steps to support the operationalization of the framework across the Ministry in the short, medium and long term.

1.2 Audience

This document is intended for any person within the Ministry who works with Ministry data and is seeking information regarding the Ministry’s data governance model. It is specifically targeted at individuals who are members of the IMG Committee and/or who fulfil one of the roles within the framework (e.g., Data Officers, Data Stewards, Data Service Providers, etc.). It should be used to guide organizational, process and technology decisions that will impact the way the Ministry leverages information as an asset. In particular, any parties who are seeking to implement a new process or technology that may impact how information is collected, used, retained, destroyed, reported or managed should understand and align to this document.

1.3 Scope

The data governance initiative that resulted in the development of this handbook was intended to establish the foundational elements of the Ministry’s data governance framework. As a result, the objective was to establish key definitions, principles, roles and responsibilities and processes for foundational data governance activities. These elements will support the piloting and eventual launch of the framework, and they will be the foundation upon which the framework will evolve to take on additional data governance functions and responsibilities.

.

¹ Ministry of Health 2010/11 - 2012/13 Service Plan (March 2010).

2 Data governance defined

The Ministry defines “data governance” as the framework that promotes roles, responsibilities, processes, standards and policies to ensure the consistent and transparent management, maintenance, and utilization of Ministry data, while mitigating risk.

A data governance program establishes information-centric processes and structures across the organization to ensure clarity regarding roles, responsibilities and decision-making processes related to information. Employing a data governance framework and instilling the discipline required to maintain it requires significant and sustained executive sponsorship, business collaboration and change management. In addition, processes related to issue management, monitoring and committee meeting preparation, logistics and follow up are required to support execution.

The Ministry’s data governance framework is based on a set of guiding principles which establish the objectives for the Ministry’s Data Governance Framework and will serve to guide planning and decision-making. The Ministry’s data governance principles are outlined below:

- **Principle 1:** The Ministry values and respects data as an asset
- **Principle 2:** Individuals understand their accountabilities for data
- **Principle 3:** The Ministry collects, uses and discloses data for purposes consistent with its mandate and as authorized under applicable legislation
- **Principle 4:** Authorized users can access data in support of the operational and strategic objectives of the Ministry
- **Principle 5:** Decisions concerning data use and disclosure are made and prioritized at the appropriate level based on a transparent, consistent and risk-based decision-making process
- **Principle 6:** The Ministry uses and discloses data in the least identifiable format possible to accomplish the intended purpose
- **Principle 7:** The Ministry creates an adaptive, transparent and collaborative environment to support effective information management
- **Principle 8:** Data quality and consistent processes support timely and effective decision making and reporting

3 Data governance framework overview

The following section provides an overview of the Ministry's data governance framework, including the Ministry's governance model and associated roles and responsibilities.

3.1 Governance model overview

The Ministry's data governance model is divided into two levels: (1) executive and (2) operational (see Figure 1). Overall accountability for the Ministry's data governance strategy and priorities and endorsement of Ministry data governance policies, standards and procedures, is assigned to the IMG Committee. The IMG Committee has the authority to create supporting structures to assist in the operationalization of the Ministry's data governance framework. These include the Governance Operations Committee (GO Committee) and the Data Governance Lead (described in greater detail below).

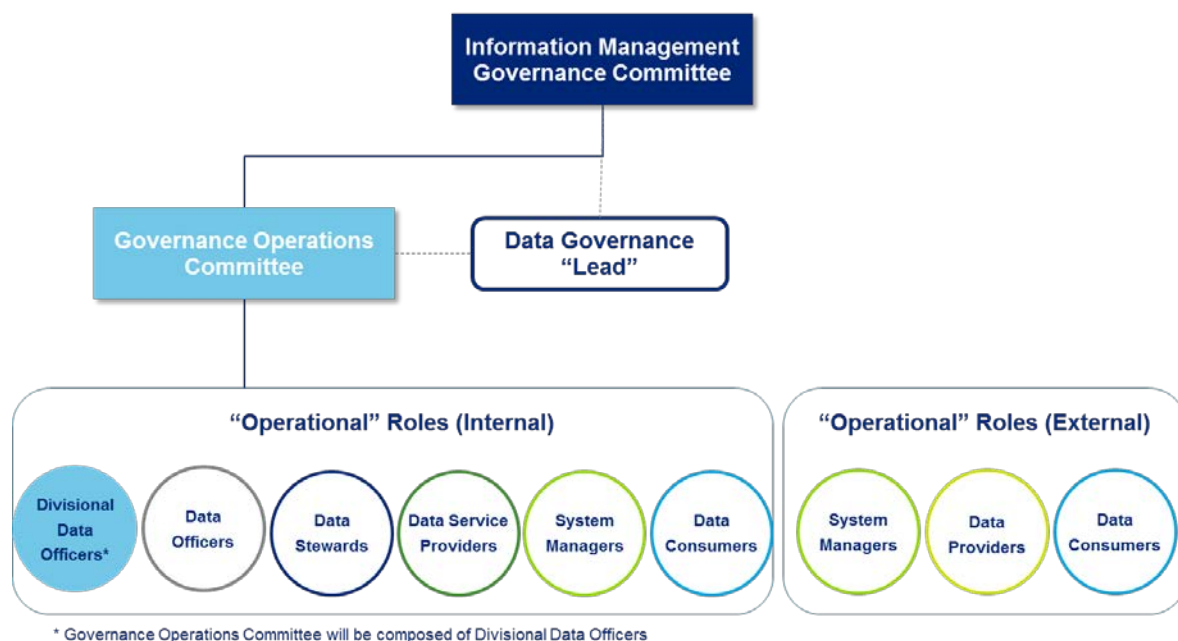


Figure 1: MOH data governance model

Figure 1 also described several operational roles that have been defined to enable the Ministry's day-to-day interactions with data including how the Ministry collects, uses, shares, retains, destroys and manages data internally and with external stakeholders.

3.2 Executive Governance Committee

The IMG Committee is a senior team of Ministry representatives responsible for overseeing, endorsing and deciding on various aspects of corporate data governance for the Ministry of Health. As illustrated in Figure 2, it is comprised of ADMs representing each of the Ministry's Divisions. The full Terms of Reference for this Committee are outlined in Appendix A, but a summary of the purpose, composition and mandate of the committee is provided below.

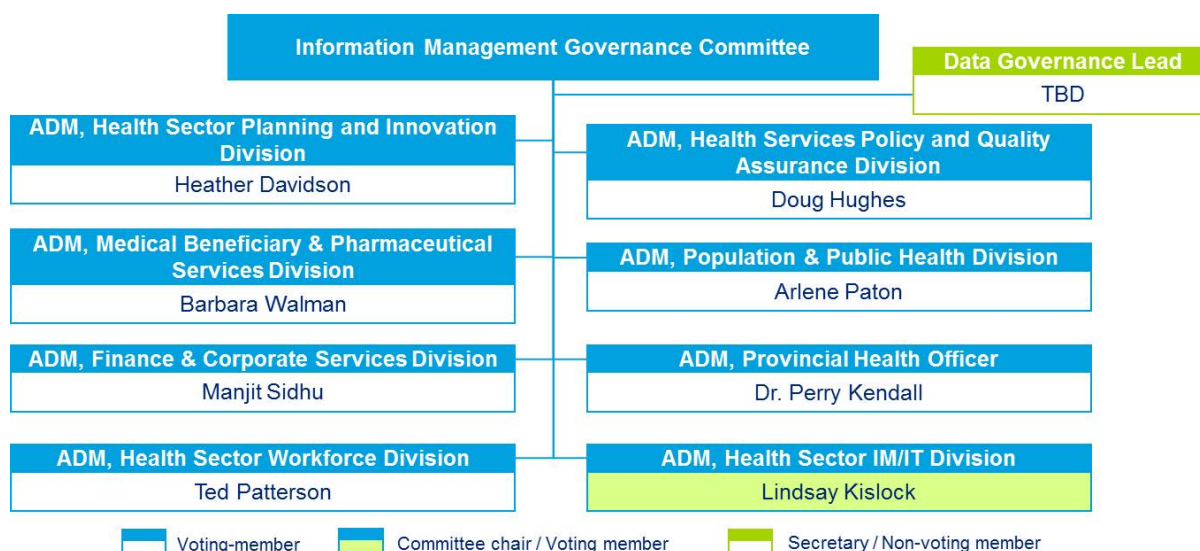


Figure 2: Information Management Governance Committee

The IMG Committee has overall responsibility and accountability for Ministry data with the objectives of providing oversight and setting direction on roles, responsibilities, processes, standards and policies as well as ensuring consistent and transparent management, maintenance and utilization of Ministry data, while mitigating risk. The extent to which these activities relate to analytics will be determined as the update to the Ministry's analytics strategy is completed. Areas of specific focus under this mandate include: data terminology, quality, protection, technology and management.

The IMG Committee:

1. Is responsible for setting Ministry direction and strategy in relation to information management and data governance, including the provision of strategic direction in relation to utilizing Ministry data as a corporate asset (with respect to risk mitigation and business enablement)
2. Defines data governance strategic priorities
3. Establishes, endorses and reviews the Ministry's data governance policies and standards
4. Is accountable for the Ministry's overall compliance with information management policy and legislation
5. Manages and approves the Ministry's investment in data assets that impact multiple Divisions
6. Allocates Data Officer (DO) resources to the Governance Operations (GO) Committee and to data-related initiatives on a priority basis
7. Provides direction to GO Committee and DOs, as required
8. Serves as the final decision-making body for escalated Data Governance issues and decisions
9. Establishes KPIs for measuring and reporting on the management of and compliance with the Data Governance Framework.

3.3 Supporting roles and structures

In order to support the deployment and ongoing operation of the governance model, the IMG Committee requires program support (Data Governance Lead) and subject matter expertise, as well

as an operational team focused on day-to-day operational data governance matters (Governance Operations Committee). These are described in greater detail below.

Data Governance Lead

A Data Governance Lead will be appointed by and accountable to the Chair of the IMG Committee. The Data Governance lead will be the most senior individual in the organization with accountability for data governance. The Data Governance Lead will support decision making within the IMG Committee and GO Committee, as well as the execution of their respective mandates, as described below.

The scope of responsibilities of the Data Governance Lead includes:

1. Supporting the effective implementation of the Data Governance Framework
2. Supporting the development of governance policy, standards and processes and ensuring alignment with corporate and/or government policies, standards and processes
3. Managing all aspects of day-to-day data governance activities including communications, measurement and reporting
4. Reviewing and advising on Executive decisions for data governance initiatives
5. Managing the GO Committee project portfolio
6. Serving as the secretary to the IMG Committee and the GO Committee
7. Supporting operational reporting on data governance metrics.

Governance Operations Committee:

The IMG Committee will assign tasks to DOs (see Operational data governance roles below) individually and collectively, through the GO Committee, in order to operationalize the Data Governance Framework and address governance-related priorities.

The IMG Committee can delegate the following types of data-related decisions and activities to the GO Committee:

- Representing the data interests of respective Divisions in the delivery of the Ministry's strategic and operational objectives
- Defining, prioritizing and operationalizing a portfolio of data-related projects that address strategic priorities set by the IMG Committee
- Raising and resolving key operational data issues and decisions in relation to data terminology, quality, protection, technology and management
- Providing recommendations to the IMG Committee on responsibilities, processes, standards and policies in relation to Ministry data as well as key data governance issues, risks and decisions
- Providing periodic reporting on the project portfolio
- Escalating risks/decisions to the IMG Committee
- Supporting IMG Committee decision-making on escalated issues by preparing decision support material and presenting to the Committee as required
- Periodic reporting to the IMG Committee that addresses data-related KPIs (i.e. quality, training, project progress, DSAs, etc.).

Additional Committee Members

In addition to the DO's from each Division, other individuals may be identified to participate in the IMG or GO Committees, including for example, individuals who can provide direct input or guidance in the areas of privacy, information security, analytics, research, vital statistics or other subject areas. These members may be appointed to both the IMG Committee and the GO Committee on an ad-hoc or permanent basis as agreed to by all members of the respective committees.

3.4 Operational data governance roles

The Ministry has developed the following operational data governance roles: data officers, data stewards, data service providers, system managers (internal and external), data consumers (internal and external) and data providers (external to the Ministry). These operational roles allow for the identification of responsibilities based on the ways in which individuals interact with data within the Ministry. The objective of these roles is to:

1. Support a common understanding of accountabilities for data-related activities;
2. Support improved efficiency and productivity through standard and repeatable business processes; and
3. Reduce risk by ensuring data is adequately and consistently protected.

It is important to note that individuals may have multiple data governance roles that they function in at any point in time.

Data Officers:

Members of the IMG Committee are responsible for identifying a senior individual to serve as their Data Officer (DO). DOs will represent the Division's interests in relation to data management and governance and serve as the accountable party for ensuring that data governance requirements, including principles, policies and standards, are operationalized within their Division. DOs will be accountable for their Division's interactions with data; including data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction).

Although the DO would have overall accountability for data governance within a Division, s/he may delegate data governance activities to Data Officers and Data Stewards within their Division to support them in operationalizing their mandate, as needed. The appointment of Data Officers may be done by branch, or other organizational unit at the discretion of the DO. Data Officers will also collaborate as the primary members of the GO Committee.

The scope of responsibilities of DOs includes:

- Responsibility for the Division's interactions with data, including data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction)
- Responsibility for developing the Division's data governance operations model
- Act as a single point of contact for their Division in relation to the following:
 - Appropriate use of data within the division
 - The escalation point for reporting and resolving data issues
 - Cross Ministry liaisons with other members of the GO Committee to review and assess common/shared data issues
 - Manage and be accountable for enterprise and division-specific data governance project portfolio
 - Recommend actions to be taken to resolve data issues
 - As required, inform or be a direct participant in work packages / projects with respect to data domains
 - Develop implementation plans for data-related projects within their division to address priorities set by IM Governance Committee
 - Report on progress against action plans
- Coordination of periodic meetings with appointed Data Officers to set Divisional strategic priorities, report on progress, and identify any issues/risks
- Escalating Divisional data-related issues, risks/decisions to the GO Committee, as needed

Data Officers (delegated):

As noted above, DO's may appoint Data Officers within their Divisions to support them in operationalizing their mandate. The scope of responsibilities of appointed Data Officers includes:

- Responsibility to support the DO in the operationalization of the various data governance activities outlined above, as assigned to the Data Officer(s)
- Supporting, as needed, the implementation of data-related initiatives
- Attending recurring meetings with DO and peers
- Escalating Divisional data-related issues, risks and decisions to the DO
- Reporting on operational governance activities and progress against action plans

Data Stewards:

Data Stewards are accountable for the management of data repositories or data products. Examples include databases, linked datasets, reports and repositories (e.g., LAN folders). Data Steward responsibilities include access management (i.e. requests/reviews for individual systems/repositories) and ensuring compliance of data set controls with applicable policies (i.e. data security, Information Sharing Agreements, privilege management, etc.). Data Steward responsibilities may be limited to an individual file or extract, which will reduce or eliminate administrative stewardship requirements, and result in only a requirement to protect data in compliance with applicable requirements. To reflect this, Data Steward responsibilities are divided into two levels as outlined in the table below:

Data Source	Responsibilities	Examples
Level 1: Source Data – Core Repositories	<ul style="list-style-type: none"> Administrative: manage access rights and related controls (access approvals and access reviews) Use and protect data in compliance with the Ministry's contractual obligations, legislative requirements and policies and standards 	<ul style="list-style-type: none"> Database Data Warehouse Linked dataset
Level 2: Operational Data / Data Products	<ul style="list-style-type: none"> Use and protect data in compliance with the Ministry's policies and standards as well as legislative requirements 	<ul style="list-style-type: none"> Paper, PDF, XLS, DOC SAS files or other large files/extracts

Data Service Providers:

Data Service Providers are individuals who receive requests for data and related analysis and data processing activities (e.g., dataset linkage). These requests can be received from internal or external stakeholders and require Data Service Providers to extract information (from a system or from multiple systems and/or datasets), manipulate it, prepare it and distribute it to the requestor (Data Consumer). They are required to know their responsibilities with respect to providing data in compliance with the Ministry's policies and standards as well as the Ministry's legislative and contractual obligations.

System Managers:

System Managers manage the Ministry's systems and technology infrastructure. System managers are responsible for the maintenance of IT infrastructure in compliance with Ministry policy on behalf of one or more divisions. This can include the management of software, tools or hardware that support data protection (e.g., through logging, access management and/or related activities). System Managers can also provide technical expertise for data-related initiatives where automated controls or tools could support information protection and compliance with the Ministry's information security and privacy policies.

Data Consumers:

Data Consumers are the end users of data and can be either internal or external to the Ministry. Data consumers are responsible for adhering to applicable Ministry data policies and processes. Data consumers are categorized into 3 areas depending on their level of data interaction:

- Highly facilitated** – individuals consume reports, dashboards and other "prepackaged" data
- Moderately facilitated** – Individuals can generate reports and content based on structured and often predefined report parameters
- Raw data** – Individuals can directly interact with data and manipulate it, link it and otherwise create value through it in a variety of ways (e.g. economic modeling, analytics, etc.)

Data Providers:

Data Providers are health care providers and organizations who provide data to the Ministry (e.g., Health Authorities, Statistics Canada, CIHI, etc.)

Communities of Practice:

To support implementation of these roles and responsibilities, and to enable sharing of lessons learned and support continual improvement, Communities of Practice associated with each of the operational roles are recommended. These groups could provide a mechanism to engage individuals fulfilling these roles across the Ministry to support information sharing, improvements in business processes and updates to responsibilities as defined in this framework. These communities could also support the GO Committee as it addresses specific issues or decisions relating to these operational roles.

4 Supporting processes

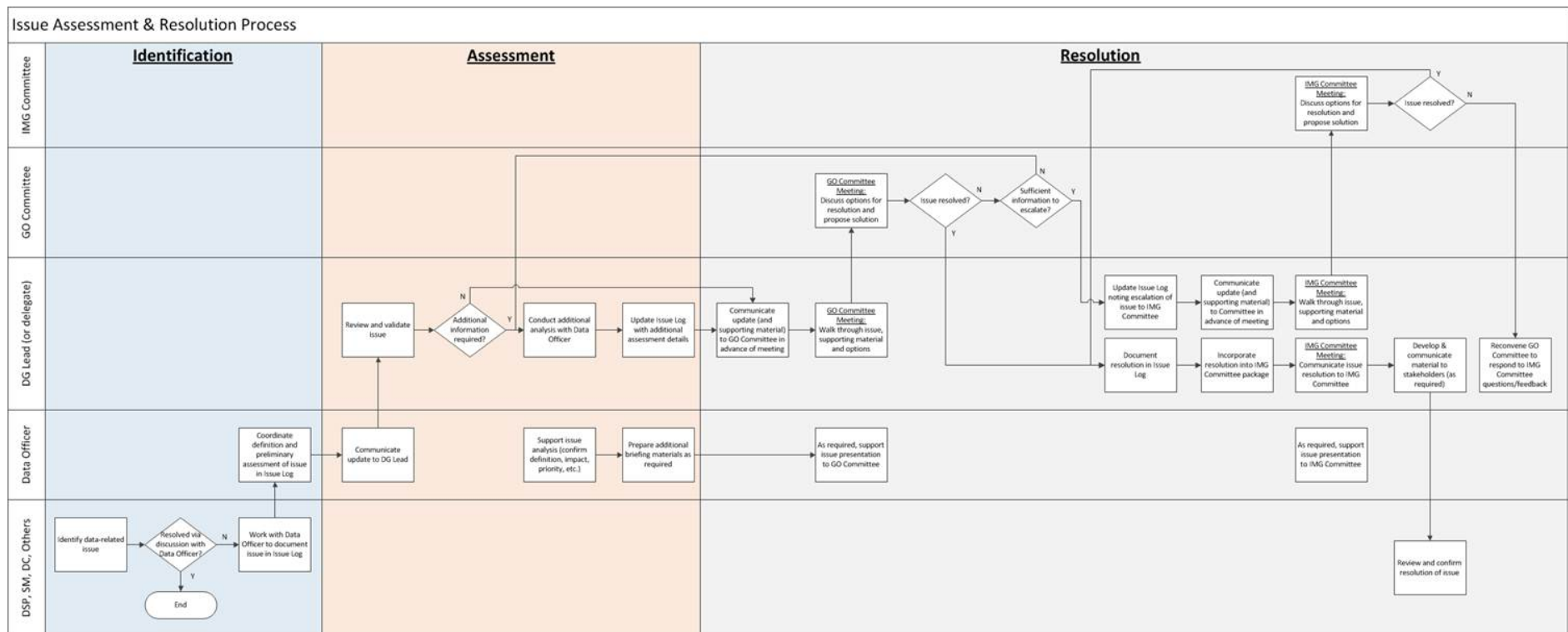
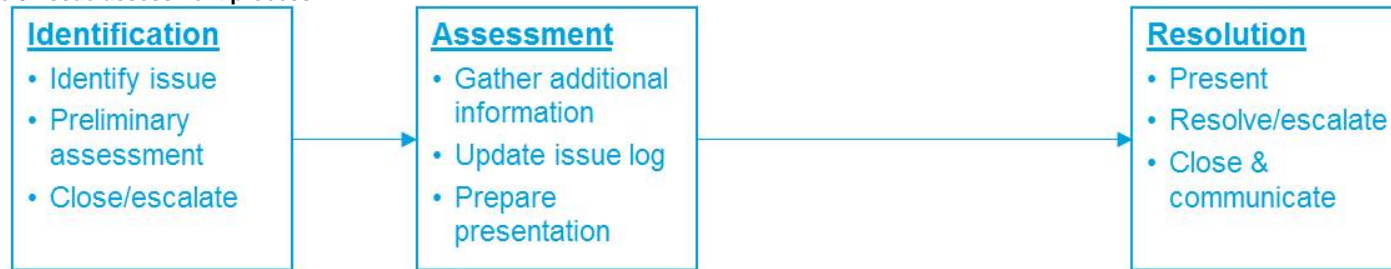
This section provides an overview of the issue assessment process to support the governance model once implemented. It addresses how issues are identified, brought forward to the GO Committee, escalated (as required), tracked and resolved.

4.1 Issues Assessment Process

The purpose of this process is to provide a mechanism for data-related issues to be identified, consistently documented, assessed, resolved or escalated as required. As these issues get prioritized for resolution, they may get passed down in the form of work packages for further analysis or resolution with the appropriate individuals. Collection of these issues will be a responsibility of the office of the Data Governance Lead.

As noted in Figure 3, the process involves the identification of an issue by an end user, business owner, or IT representative. Once the issue is identified and reported, the Data Officer will support preliminary review and seek to resolve the issue at that time. If resolution is not possible, the issue will be documented in the issue log and communicated to the office of the Data Governance Lead. At this point, the impact and criticality of the issue is confirmed (through further dialogue with Divisional representatives as required), and additional information is gathered to support the evaluation of the issue and options for remediation. The issue is then reviewed with the GO Committee, and if resolution is not possible, it is escalated to the IMG Committee.

Figure 3: Issue assessment process



5 Deployment

The following table outlines a series of next steps to support the deployment of the data governance framework (as at July, 2013). It is designed to highlight the key activities, outcomes and risks associated with short, medium and long-term deployment phases. The focus in the short term is to operationalize and assign individuals to the data governance committees, supporting structures and operational roles. In the medium term, the focus of the governance model is to support the implementation of key Phase 2 projects, as well as to identify key data governance issues for analysis, resolution or escalation. In Phase 3, there is a transition to a more strategic focus for the model; however, the operational activities initiated in Phase 2 will continue.

Immediate (Jul – Aug) “Establish DG Infrastructure”	Medium term (Sep – Dec) “Oversee Phase 2/3 Projects”	Ongoing (Jan 2014 onward) “Ongoing Operations”
Activities		
<ul style="list-style-type: none"> • Identification of DOs (ADMs) • Complete Data Governance Playbook • Develop training and onboarding material for DOs (DG Lead) • Train DOs (DG Lead) • Support DOs in developing implementation model (DG Lead) • Identify and onboard support resources (DG Lead) • Issue DG Update to the Ministry about this initiative and identifying DOs (DG Lead) 	<ul style="list-style-type: none"> • Focus initially on management and oversight of key Phase 2 projects (e.g., Condor transition) • Catalogue and prioritize operational DG issues (GO Committee) • Facilitate resolution of DG issues and escalate for approval or resolution (GO Committee) • Develop key KPIs (e.g., compliance, training) (DG Lead) 	<ul style="list-style-type: none"> • Establish strategic Data Governance Priorities (IMG Committee) • Consider expanding scope of DG function to include or support other key data elements such as architecture, quality, analytics (IMG Committee) • Review and update to DG-related policies and guidelines (GO Committee) • Confirm full-time ongoing Data Officers and supporting resources
Benefits / Outcomes		
<ul style="list-style-type: none"> • Established framework for Business/IT collaboration for implementation of Category 2 & 3 projects • Central point of coordination for issues, risks and decisions related to data • Fully resourced DG support structure 	<ul style="list-style-type: none"> • Operational decision-making framework for projects and high priority DG issues • Visibility into real-time project issues and decisions • Issues and decisions identified, tracked and resolved at the right level • Ability to track and report progress internally and externally 	<ul style="list-style-type: none"> • DG priorities are clearly identified, communicated and incorporated into strategic and operational plans • Permanent Data Officers assigned and operational • Operational decision-making framework for projects • Visibility into real-time project issues and decisions • Issues and decisions identified, tracked and resolved at the right level
Risks		
<ul style="list-style-type: none"> • Loss of momentum in early stages • Conflicting priorities for Data Officers as this is added to existing responsibilities 	<ul style="list-style-type: none"> • Potential for decision-making process to be overwhelmed due to scale of change • Potential for conflicting decisions if dependencies are not clearly assessed and defined 	<ul style="list-style-type: none"> • Potential fatigue arising from Category 2 & 3 projects • Potential loss of momentum and desire to return to “business as usual” and decentralize decision-making

6 Data governance glossary

The data governance glossary serves as the official glossary of terminology used in the Ministry Data Governance program. This glossary applies to all terminology appearing in the Data Governance Program's policies, procedures, and models.

Term	Description
Control	A means of managing a risk or ensuring that an objective is achieved. Controls can be preventative, detective, or corrective and can be fully automated, procedural, or technology-assisted human-initiated activities. They can include actions, devices, procedures, techniques, or other measures.
Data Governance	"Data Governance" is the framework that promotes roles, responsibilities, processes, standards and policies; to ensure the consistent and transparent management, maintenance, and utilization of Ministry data while mitigating risk.
Data Governance Model	Refers to how data governance actually works within the Ministry. It includes an organization structure, roles and responsibilities, interaction model, standards and processes. This model is reviewed for efficiency and effectiveness on a periodic basis and is the on-going mechanism to execute the data governance strategy.
Data Governance Framework	The overall effort to institute and maintain data governance at the Ministry, which includes all members of the Data Governance Organization as well as all policies, procedures, artefacts, etc. used in its implementation.
Data Retention and Archiving	The capability to appropriately retain and archive data to comply with laws, regulations and corporate data life cycle policies.
Data Quality	<p>The business value of data as assessed by its accuracy, integrity, completeness, consistency, and uniqueness.</p> <ul style="list-style-type: none"> • Accuracy – The actual correctness and validity of the data, such that the data reflects "real world" values. Precision is also a component of accuracy. Accuracy plays a major part in data being reconcilable • Completeness – The state of being free from missing data (e.g. lacking a value in a required field, or lacking entire rows altogether) or partial data (e.g. a street address without the primary address number). • Integrity – Critical to the trustworthiness of data, integrity is the assurance that data is intact and correct. It means confidence that data has not been modified in either an unauthorized or undesired way. Integrity also refers to preservation of relationships between objects or data points, such as the hierarchical relations of legal entities. • Consistency – Relies on data standards for assurance that data always conforms to the expected form. An example of inconsistency would be the alternating use of "Street", "St.", "ST", and "street" in an address field. • Uniqueness – Relates primarily to elimination of duplicate records. For example, if a given customer exists with slightly differing names in multiple different records, this is a uniqueness problem. Secondly, uniqueness ties into the ability to correctly identify and match records for a single entity that exists in multiple systems, such as a particular customer that has records in multiple different databases.
Domain (Data Domain)	A data domain is a functional area or business unit to which responsibilities over data apply. "Domain" may refer to a specific data domain (e.g. prescription data or medical services claims data) or, in some cases, a broader subject area (other data such as rules or metrics).
Enterprise Data	Data that is defined and structured for use across the entire organization. This is in contrast to "local" or "silo" data, which has meanings specific to the group that uses it.

Term	Description
Enterprise Data Management	A holistic approach to managing all of an organization's data.
Master Data	Master Data refers to the "nouns" upon which transactions take action. Master Data describes core entities of an organization that are used by multiple business process and IT systems. Examples are parties (e.g., patients, employees, vendors, suppliers), places (e.g., locations, regions, offices), and things (e.g., accounts, services provided, etc.).
Master Data Management (MDM)	A structured approach to defining and managing an organization's Master Data. It is the management of the information required to create and maintain an enterprise-wide "system of record" for core entities, in order to capture business transactions and measure results.
Metadata	Simply put, metadata is any data about data. It is data that describes the structure of data or meta objects. Business metadata provides documentation about all elements contained in the system such as definitions, business rules, valid values, data classifications, data usage, data lineage, etc. Business metadata defines the information in a business or operational context. Technical metadata provides the description of metadata within IT.
Policy	A formal statement of direction that enacts or gives authority for use, management and oversight of enterprise resources.
Procedure	A document containing steps that specify how to perform a process.
Remediation Plan	The detailed analysis and set of resolution steps that must be performed to satisfactorily resolve a data quality issue.
Retention	Defines a data type's "shelf life" - after which data is archived or destroyed.

Appendix A: Information Management Governance Committee Terms of Reference

Information Management Governance Committee

Terms of Reference

A. PURPOSE

The Information Management Governance Committee (IMG Committee)² is a senior team of Ministry representatives responsible for overseeing, endorsing and deciding on various aspects of corporate data governance for the Ministry of Health.

The IMG Committee's areas of responsibility include:

- Defining the strategy for Ministry of Health data governance;
- Prioritization and resource allocation for initiatives related to data management;
- Endorsement of data management policies (including those related to data terminology, quality, protection, technology and management); and
- Ensuring compliance mechanisms are in place to monitor and verify adherence to data management policies and regulatory requirements.

Furthermore, the IMG Committee is accountable for operationalizing the following data governance principles of the Ministry of Health through their decision making and policy setting activities:

- **Principle 1:** The Ministry values and respects data as an asset
- **Principle 2:** Individuals understand their accountabilities for data
- **Principle 3:** The Ministry collects, uses and discloses data for purposes consistent with its mandate and as authorized under applicable legislation
- **Principle 4:** Authorized users can access data in support of the operational and strategic objectives of the Ministry
- **Principle 5:** Decisions concerning data use and disclosure are made and prioritized at the appropriate level based on a transparent, consistent and risk-based decision making process
- **Principle 6:** The Ministry uses and discloses data in the least identifiable format possible to accomplish the intended purpose
- **Principle 7:** The Ministry creates an adaptive, transparent and collaborative environment to support effective information management.
- **Principle 8:** Data quality and consistent processes supports timely and effective decision making and reporting

B. SCOPE AND RESPONSIBILITIES

The Committee has overall responsibility and accountability for Ministry data with the objectives of providing oversight and setting direction on roles, responsibilities, processes, standards and policies as well as ensuring consistent and transparent management, maintenance and utilization of Ministry data while mitigating risk. The extent to which these activities relate to analytics will be determined as the update to the Ministry's analytics strategy is completed. Areas of specific focus under this mandate include: data terminology, quality, protection, technology and management.

² "Information management" refers to the collection, use, disclosure, retention, destruction, protection, quality and availability of Ministry data.

In Scope:

The IMG Committee:

1. Responsible for setting Ministry direction and strategy in relation to information management and data governance, including the provision of strategic direction in relation to utilizing Ministry data as a corporate asset (with respect to risk mitigation and business enablement);
2. Defines data governance strategic priorities;
3. Establishes, endorses and reviews the Ministry's data governance policies and standards;
4. Is accountable for the Ministry's overall compliance with information management policy and legislation;
5. Manages and approves the Ministry's investment in data assets that impact multiple Divisions;
6. Allocates Data Officer resources to the Governance Operations (GO) Committee and to data-related initiatives on a priority basis;
7. Provides direction to Governance Operations Committee and Data Officers, as required;
8. Serves as the final decision-making body for escalated Data Governance issues and decisions; and
9. Establishes KPIs for measuring and reporting on the management of and compliance with the Data Governance Framework.

With respect to financial information, it should be noted that the Office of the Comptroller General establishes policies for financial systems (defined in CPPM Ch. 13 see s.13.3) and for communication of financial control standards. In all ministries the Executive Financial Officer has core policy accountabilities for financial systems as articulated in Chapter 13 of CPPM.

C. MEMBERSHIP

The Committee is comprised of the most senior representatives of the each Division (ADM) with authority to act on behalf of their respective organizations. The Chair of the Committee is a position held by one of the Committee members and is appointed by the Committee (based on a majority vote) on an annual basis. The Data Governance Lead (see below for additional detail) will serve as the secretary for the Committee and will participate in the Committee as a non-voting member. This role will also be appointed by the Committee, but will not change annually.

D. SUPPORTING STRUCTURES

Data Governance Lead

A Data Governance Lead will be appointed by and be accountable to the Chair of the IMG Committee. The Data Governance lead will be the most senior individual in the organization with accountability for data governance. The Data Governance Lead will support decision making within the IMG Committee and Governance Operations Committee, as well as the execution of their respective mandates, as described below.

The scope of responsibilities of the Data Governance Lead includes:

- Supporting the effective implementation of the Data Governance Framework
- Supporting the development of governance policy, standards and processes and ensuring alignment with corporate and/or government policies, standards and processes
- Managing all aspects of day-to-day data governance activities including communications, measurement and reporting
- Reviewing and advising on Executive decisions for data governance initiatives
- Managing the GO Committee project portfolio
- Supporting operational reporting on data governance metrics.

These responsibilities may be amended from time to time by the IMG Committee.

Governance Operations Committee

Members of the IMG Committee are responsible for identifying a senior level staff member to serve as their Division's Data Officer. Data Officers (DOs) will represent each Division's interests in relation to data management and governance and serve as the accountable party for ensuring that data governance requirements, including principles, policies and standards, are operationalized within their Division. DOs will be accountable for their Division's interactions with data; including, data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction). Although a DO would have overall accountability for data governance within a Division, s/he may delegate data governance activities to other team members, as needed. DOs may delegate to Data Stewards and may also identify "Data Officers" within their Divisions to support them in this role. DOs will collaborate through the Governance Operations (GO) Committee.

The IMG Committee will assign tasks to DOs individually and collectively, through the GO Committee, in order to operationalize the Data Governance Framework and address governance-related priorities. The IMG Committee can delegate the following types of data-related decisions and activities to the GO Committee:

- Representing the data interests of respective Divisions in the delivery of the Ministry's strategic and operational objectives
- Defining, prioritizing and operationalizing a portfolio of data-related projects that address strategic priorities set by the IMG Committee
- Raising and resolving key operational data issues and decisions in relation to data terminology, quality, protection, technology and management
- Providing recommendations to the IMG Committee on responsibilities, processes, standards and policies in relation to Ministry data as well as key data governance issues, risks and decisions
- Providing periodic reporting on the project portfolio
- Escalating risks/decisions to the IMG Committee
- Supporting IMG Committee decision-making on escalated issues by preparing decision support material and presenting to the Committee as required
- Periodic reporting to the IMG Committee that addresses data-related KPIs (i.e. quality, training, project progress, DSAs, etc.)

Additional Committee Members

In addition to the DO's from each Division, other individuals may be identified to participate in the IMG or GO Committees, including for example, individuals who can provide direct input or guidance in the areas of privacy, information security, analytics, research, vital statistics or other subject areas. These members may be appointed to both the IMG Committee and the GO Committee on an ad-hoc or permanent basis as agreed to by all members of the respective committees.

E. DECISION-MAKING PROTOCOLS

Quorum

A quorum constitutes 50% plus 1 of the members.

Decisions/Voting

Decisions are by consensus on matters of policy and procedure whenever possible. If not possible, decisions are by a 2/3 majority vote of the members, including those not present at the meeting.

Escalation

The IMG Committee will act as the final authority for decisions on items escalated from the Governance Operations Committee. The Governance Operations Committee will be the primary mechanism through which these items will be identified, assessed, prioritized and escalated as required. Examples of triggers for escalation to the IMG Committee include those items where:

- There are significant cross-Divisional or Ministry-wide data, financial or resource implications (as determined by the Governance Operations Committee)
- Questions of strategic importance to the Ministry around data governance
- There is a question of prioritizing limited resources against significant cross-divisional initiatives

- There are decisions concerning data governance policy, where recommendations may be made by the Governance Operations Committee, but decisions concerning endorsement of policy must occur through the IMG Committee
- There are significant changes proposed to the IMG Committee's Terms of Reference or mandate or to those of other key data governance roles (Data Governance Lead or Data Officers)

It should be noted that, in the case of high-risk or time-sensitive matters, it is possible that an ad-hoc meeting of the IMG Committee can be called to brief the Committee and obtain Executive guidance as required.

F. MEETING LOGISTICS

Frequency of meetings

IMG Committee meetings will be held on a monthly basis. Ad-hoc meetings may be scheduled on an exception basis as required to address high-risk or urgent data-related matters.

Standing agenda

The Data Governance Lead will manage the agenda with direction from the Chair. All Committee members may request additions or changes to the agenda as required. Typical agenda items for discussion will include:

- a) Chair's introduction
- b) Review of minutes and actions arising from the last meeting
- c) Review of decision log and associated supporting material (where appropriate)
 - a. Outstanding items
 - b. New items
 - c. Delegated items (updates to the IMG Committee as required)
- d) Strategic data governance items (the following key topics are proposed to be included in the agenda on an as-needed basis)
 - a. Data quality
 - b. Data protection
 - c. Data management
 - d. Technology
 - e. Terminology
- e) Confirmation of outstanding decisions and action items
- f) Date of next meeting

G. DELIVERABLES AND SUPPORTING DOCUMENTATION

Strategic Plan

The IMG Committee will be responsible for defining, on an annual basis, the strategic priorities of the Ministry with respect to information management. This strategic plan will provide guidance to the GO Committee regarding strategic priorities and associated projects for which they will be accountable. These priorities will also support decision-making related to investment and resource allocation by the GO and IMG Committees.

Decision support materials

The Data Governance Lead (or delegate) will be responsible for collating and circulating materials required to support deliberation and decision-making by the IMG Committee. GO Committee members will support preparation of these materials (issue definition, option analysis and evaluation and recommendations) and they will be circulated no later than 7 days prior to each IMG Committee meeting. These materials may be presented by the appropriate GO Committee members and will be retained for future reference and maintained by the Data Governance Lead.

Meeting minutes

The Data Governance Lead (or delegate) will take minutes of each meeting, and will prepare and distribute meeting documents, including minutes, electronically no later than 7 working days in advance of each meeting.

Draft minutes will be tabled for review and approval at the next meeting. As appropriate, reasons for decisions may be recorded in minutes; but only decisions, not dissenting opinions, will be recorded. The results of a vote will be recorded only as approved/not approved.

Issue/Decision Log

The Data Governance Lead will be responsible for creating and managing a formal log to record, track and report on data governance issues and decisions. The GO Committee, with the support of the Data Governance Lead (or delegate), will actively manage this log. It will be used to communicate decisions or issues resolved by the GO Committee to the IMG Committee (for information purposes), and to track those items that require escalation in order to be resolved.

H. REPORTING PROTOCOL

The Committee, with assistance from the Data Governance Lead, will report to the Deputy Minister responsible at least once per year regarding the activities of the Committee.

Issue Assessment & Resolution Process



Divisional Data Officer Role

Finance and Corporate Services Division



August 28, 2013

Agenda

- Review DDO responsibilities
- Discuss FCSD-specific considerations for governance model
- Discuss training requirements
- Next steps

Divisional Data Officer Responsibilities

Divisional Data Officers

Mandate

Responsible for a Division's interactions with data, including data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction).

Expectation of Role

- This role would require a significant investment of time from a senior staff person with a detailed understanding of division operations and management of data.
- Time required to fulfill obligations of role will vary by Division depending on amount of data administered and complexity of data use.
- Although the Divisional Data Officer would have overall accountability for data governance, they may delegate data governance activities to other team members, as needed

Divisional Data Officer – Job Description

Responsibilities

- Responsible for the Divisions interactions with data, including data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction).
- Proactively supports and represents their Division with respect to matters involving data, including:
 - Appropriate use of the data within the division (in accordance with policy and legal requirements)
 - Acting as an escalation point for reporting and resolving data issues and questions
 - Representing the interests of their Divisions at the GO Committee and liaising with other members of the Committee to review and assess common/shared data issues
 - Managing and being accountable for enterprise and division-specific data governance project portfolio
 - Developing implementation plans for the data governance model within their division to address priorities set by IM Governance Committee
 - Report on progress against action plans
- Communication of data governance decisions out to their Divisions, as appropriate.

Skills and Knowledge

- Problem solving complex data interactions including risk and value impact analysis and prioritization.
- Ability to liaise with technical staff and translate technological data circumstance to business terms.
- Good understanding of data lifecycle and usage within their division, including processes for data origination, processing and controls.

Measurements

- Attendance and participation in GO Team meetings as reflected in the minutes and communications.
- On time completion of data governance portfolio projects
- Number of data issues for their division that have been analyzed and resolved.
- Satisfaction of division stakeholders being represented measured through quarterly survey and data community testimonials.
- Data governance score card with defined performance metrics for the division.

Division-specific requirements

FCSD Data Environment

Finance and Corporate Services (FCS) Division System Inventory Model
Accounting and Operations (AO)

Collection

Use

Disclosure

s. 15

Last updated: 18-Jan-2013

FCSD Data Environment (2)

Finance and Corporate Services (FCS) Division System Inventory Model
Audit and Investigations (A&I)

s. 15

Last updated: 18-Jan-2013

Key characteristics of the environment

- Data environment:
 - For certain branches, there is a significant amount of PI received, managed locally and in some cases, shared with third parties
 - PI is stored in electronic form (within the FCSD LAN) and paper form (in locked filing cabinets)
 - There do not appear to be any significant, locally-managed data sets (to be confirmed)

Considerations for governance model implementation

- The Division requires representation at the GO Committee to ensure:
 - FSCD interests, risks and issues are identified and communicated
 - Key data-related decisions address FCSD perspectives and priorities
- It may be appropriate to consider Branch-level Data Officers for branches with significant PI (Accounting Operations and Audit & Investigations)
- There does not appear to be a need for dataset stewards as there are no identified locally-managed datasets (to be confirmed)

Training

Training requirements

- Training will be targeted at DDOs to ensure a consistent level of understanding regarding Data Governance and relevant roles and responsibilities
- Feedback is being sought from all DDOs regarding training requirements and key topics to include

Key next steps

Next steps

- Confirm Divisional data governance “team members” based on Divisional requirements
- Delivery of training
- Transition to GO Committee (from ED Working Group)
- Initial focus on Phase 2 project oversight and support
- Working with GO Committee, identify high-priority issues and decisions that require Committee review (and escalation where required)

Deloitte.

Divisional Data Officer Role

Health Authorities Division



August 22, 2013

Agenda

- Review DDO responsibilities
- Discuss HAD-specific considerations for governance model
- Discuss training requirements
- Next steps

Divisional Data Officer Responsibilities

Divisional Data Officers

Mandate

Responsible for a Division's interactions with data, including data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction).

Expectation of Role

- This role would require a significant investment of time from a senior staff person with a detailed understanding of division operations and management of data.
- Time required to fulfill obligations of role will vary by Division depending on amount of data administered and complexity of data use.
- Although the Divisional Data Officer would have overall accountability for data governance, they may delegate data governance activities to other team members, as needed

Divisional Data Officer – Job Description

Responsibilities

- Responsible for the Divisions interactions with data, including data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction).
- Proactively supports and represents their Division with respect to matters involving data, including:
 - Appropriate use of the data within the division (in accordance with policy and legal requirements)
 - Acting as an escalation point for reporting and resolving data issues and questions
 - Representing the interests of their Divisions at the GO Committee and liaising with other members of the Committee to review and assess common/shared data issues
 - Managing and being accountable for enterprise and division-specific data governance project portfolio
 - Developing implementation plans for the data governance model within their division to address priorities set by IM Governance Committee
 - Report on progress against action plans
- Communication of data governance decisions out to their Divisions, as appropriate.

Skills and Knowledge

- Problem solving complex data interactions including risk and value impact analysis and prioritization.
- Ability to liaise with technical staff and translate technological data circumstance to business terms.
- Good understanding of data lifecycle and usage within their division, including processes for data origination, processing and controls.

Measurements

- Attendance and participation in GO Team meetings as reflected in the minutes and communications.
- On time completion of data governance portfolio projects
- Number of data issues for their division that have been analyzed and resolved.
- Satisfaction of division stakeholders being represented measured through quarterly survey and data community testimonials.
- Data governance score card with defined performance metrics for the division.

Division-specific requirements

HAD Data Environment

Health Authorities Division (HAD) System Inventory Model
Home, Community and Integrated Care (HCIC)

Collection

Use

Disclosure

s. 15

HAD Data Environment (2)

Health Authorities Division (HAD) System Inventory Model Hospital and Provincial Services Branch (HPSB)		
Collection	Use	Disclosure

s. 15

HAD Data Environment (3)

Health Authorities Division (HAD) System Inventory Model Mental Health and Substance Use (MHSU)			
	Collection	Use	Disclosure
Last updated: 18-Jan-2013			
		s. 15	

HAD Data Environment (3)

Health Authorities Division (HAD) System Inventory Model
Patient Safety and Care Quality (PSCQ)

Collection	Use	Disclosure
------------	-----	------------

s. 15

Last updated: 18-Jan-2013

Key characteristics of the environment

- Data environment:
 - Significant amount of PI used and stored across multiple branches
 - Strong reliance on P&I for analytics and reporting
 - High-volume of information sharing with Health Authorities
 - Some databases/datasets managed locally

Considerations for governance model implementation

- The Division requires strong representation at the GO Committee to ensure:
 - HAD interests, risks and issues are identified and communicated
 - Key data-related decisions address HAD perspectives and priorities
- A Branch-level Data Officer network will likely be required to support the DDO
- Given the complexity of the data environment, there is a need to ensure controls are developed and in place and that they operating in accordance with policy and legal requirements
- There is a need for dataset stewards to ensure access to datasets is appropriately managed

Training

Training requirements

- Training will be targeted at DDOs to ensure a consistent level of understanding regarding Data Governance and relevant roles and responsibilities
- Feedback is being sought from all DDOs regarding training requirements and key topics to include

Key next steps

Next steps

- Confirm Divisional data governance “team members” based on Divisional requirements
- Delivery of training
- Transition to GO Committee (from ED Working Group)
- Initial focus on Phase 2 project oversight and support
- Working with GO Committee, identify high-priority issues and decisions that require Committee review (and escalation where required)
- Work with PID team to support implementation and ongoing operation of the governance model and related controls



Divisional Data Officer Role

Medical Services & Health Human Resources



August 27, 2013

Agenda

- Review DDO responsibilities
- Discuss MSHHR-specific considerations for governance model
- Discuss training requirements
- Next steps

Divisional Data Officer Responsibilities

Divisional Data Officers

Mandate

Responsible for a Division's interactions with data, including data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction).

Expectation of Role

- This role would require a significant investment of time from a senior staff person with a detailed understanding of division operations and management of data.
- Time required to fulfill obligations of role will vary by Division depending on amount of data administered and complexity of data use.
- Although the Divisional Data Officer would have overall accountability for data governance, they may delegate data governance activities to other team members, as needed

Divisional Data Officer – Job Description

Responsibilities

- Responsible for the Divisions interactions with data, including data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction).
- Proactively supports and represents their Division with respect to matters involving data, including:
 - Appropriate use of the data within the division (in accordance with policy and legal requirements)
 - Acting as an escalation point for reporting and resolving data issues and questions
 - Representing the interests of their Divisions at the GO Committee and liaising with other members of the Committee to review and assess common/shared data issues
 - Managing and being accountable for enterprise and division-specific data governance project portfolio
 - Developing implementation plans for the data governance model within their division to address priorities set by IM Governance Committee
 - Report on progress against action plans
- Communication of data governance decisions out to their Divisions, as appropriate.

Skills and Knowledge

- Problem solving complex data interactions including risk and value impact analysis and prioritization.
- Ability to liaise with technical staff and translate technological data circumstance to business terms.
- Good understanding of data lifecycle and usage within their division, including processes for data origination, processing and controls.

Measurements

- Attendance and participation in GO Team meetings as reflected in the minutes and communications.
- On time completion of data governance portfolio projects
- Number of data issues for their division that have been analyzed and resolved.
- Satisfaction of division stakeholders being represented measured through quarterly survey and data community testimonials.
- Data governance score card with defined performance metrics for the division.

Division-specific requirements

MSHHR Data Environment

Medical Services and Health and Human Resources Division (MSHHR) System Inventory Model Medical Services Economic Analysis (MSEA) Branch			
	Collection	Use	Disclosure
Last updated: 18-Jan-2013			

s. 15

MSHHR Data Environment (2)

Medical Services and Health and Human Resources Division (MSHHR) System Inventory Model
Physician Compensation Branch and Rural Programs (PCBRP)

Collection	Use	Disclosure
------------	-----	------------

s. 15

MSHHR Data Environment (3)

Medical Services and Health and Human Resources Division (MSHHR) System Inventory Model
Diagnostic Facilities Administration (DFA)

Collection	Use	Disclosure
------------	-----	------------

s. 15

MSHHR Data Environment (4)

Medical Services and Health and Human Resources Division (MSHHR) System Inventory Model			
Medical Services Branch (MSB)			
Collection	Use	Disclosure	
			s. 15

Last updated: 18-Jan-2013

MSHHR Data Environment (5)

Medical Services and Health and Human Resources Division (MSHHR) System Inventory Model
Primary Health Care and Specialist Services (PHCS)

Collection

Use

Disclosure

s. 15

Last updated: 18-Jan-2013

Key characteristics of the environment

- Data environment:
 - Complex data environment with numerous incoming data feeds, local data sets and outgoing data feeds
 - Significant amount of PI used and stored across multiple branches
 - Advanced analytics and data management capabilities involving significant amounts of PI
 - Some significant datasets managed locally

Considerations for governance model implementation

- The Division requires strong representation at the GO Committee to ensure:
 - MSHHR interests, risks and issues are identified and communicated
 - Key data-related decisions address MSHHR perspectives and priorities
- A Branch-level Data Officer network will likely be required to support the DDO
- There may be a need for dataset stewards to ensure access to locally-managed datasets is appropriately coordinated

Training

Training requirements

- Training will be targeted at DDOs to ensure a consistent level of understanding regarding Data Governance and relevant roles and responsibilities
- Feedback is being sought from all DDOs regarding training requirements and key topics to include

Key next steps

Next steps

- Confirm Divisional data governance “team members” based on Divisional requirements
- Delivery of training
- Transition to GO Committee (from ED Working Group)
- Initial focus on Phase 2 project oversight and support
- Working with GO Committee, identify high-priority issues and decisions that require Committee review (and escalation where required)
- Work with PID team to support implementation and ongoing operation of the governance model and related controls

Deloitte.

Divisional Data Officer Role

Planning & Innovation Division



September 4, 2013

Agenda

- Review DDO responsibilities
- Discuss PID-specific considerations for governance model
- Discuss training requirements
- Next steps

Divisional Data Officer Responsibilities

Data Officers

Mandate

Responsible for a Division's interactions with data, including data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction).

Expectation of Role

- This role would require a significant investment of time from a senior staff person with a detailed understanding of division operations and management of data.
- Time required to fulfill obligations of role will vary by Division depending on amount of data administered and complexity of data use.
- Although the Data Officer would have overall accountability for data governance, they may delegate data governance activities to other team members, as needed

Data Officer – Job Description

Responsibilities

- Responsible for the Divisions interactions with data, including data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction).
- Proactively supports and represents their Division with respect to matters involving data, including:
 - Appropriate use of the data within the division (in accordance with policy and legal requirements)
 - Acting as an escalation point for reporting and resolving data issues and questions
 - Representing the interests of their Divisions at the GO Committee and liaising with other members of the Committee to review and assess common/shared data issues
 - Managing and being accountable for enterprise and division-specific data governance project portfolio
 - Developing implementation plans for the data governance model within their division to address priorities set by IM Governance Committee
 - Report on progress against action plans
- Communication of data governance decisions out to their Divisions, as appropriate.

Skills and Knowledge

- Problem solving complex data interactions including risk and value impact analysis and prioritization.
- Ability to liaise with technical staff and translate technological data circumstance to business terms.
- Good understanding of data lifecycle and usage within their division, including processes for data origination, processing and controls.

Measurements

- Attendance and participation in GO Team meetings as reflected in the minutes and communications.
- On time completion of data governance portfolio projects
- Number of data issues for their division that have been analyzed and resolved.
- Satisfaction of division stakeholders being represented measured through quarterly survey and data community testimonials.
- Data governance score card with defined performance metrics for the division.

Division-specific requirements

PID Data Environment

Planning and Innovation Division (P&I) System Inventory Model Performance Measurement, Analysis, and Reporting (PMAR) Branch			
Last updated: 18-Jan-2013	Collection	Use	Disclosure

s. 15

PID Data Environment (2)

Planning and Innovation Division (P&I) System Inventory Model
Health Information Support (HIS) Branch

	Collection	Use	Disclosure
Last updated: 18-Jan-2013		s. 15	

Key characteristics of the environment

- Data environment:
 - Complex data environment with numerous incoming data feeds, local data sets and outgoing data feeds
 - High volume of requests for data and analysis from internal and external stakeholders
 - Advanced analytics capabilities involving significant amounts of PI
 - Some significant datasets managed locally
- Role within the Ministry
 - Key role in driving analytics strategy, technology and capabilities
 - Critical support function to enable all Divisions to deliver on Ministry strategy

Considerations for governance model implementation

- The Division requires strong representation at the GO Committee to ensure:
 - PID interests, risks and issues are identified and communicated
 - Key data-related decisions address PID perspectives and priorities
- Given the breadth of the Division's data mandate, a Branch-level Data Officer network will likely be required to support the DDO
- Given the complexity of the data environment, there is a need to ensure controls are developed and in place and that they operating in accordance with policy and legal requirements
- There is a need for dataset stewards to ensure access to datasets is appropriately managed

Training

Training requirements

- Training will be targeted at DDOs to ensure a consistent level of understanding regarding Data Governance and relevant roles and responsibilities
- Feedback is being sought from all DDOs regarding training requirements and key topics to include

Key next steps

Next steps

- Confirm Divisional data governance “team members” based on Divisional requirements
- Delivery of training
- Transition to GO Committee (from ED Working Group)
- Initial focus on Phase 2 project oversight and support
- Working with GO Committee, identify high-priority issues and decisions that require Committee review (and escalation where required)
- Work with PID team to support implementation and ongoing operation of the governance model and related controls

Deloitte.

Divisional Data Officer Role

Medical Services & Health Human Resources



August 27, 2013

Agenda

- Review DDO responsibilities
- Discuss PPH-specific considerations for governance model
- Discuss training requirements
- Next steps

Divisional Data Officer Responsibilities

Divisional Data Officers

Mandate

Responsible for a Division's interactions with data, including data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction).

Expectation of Role

- This role would require a significant investment of time from a senior staff person with a detailed understanding of division operations and management of data.
- Time required to fulfill obligations of role will vary by Division depending on amount of data administered and complexity of data use.
- Although the Divisional Data Officer would have overall accountability for data governance, they may delegate data governance activities to other team members, as needed

Divisional Data Officer – Job Description

Responsibilities

- Responsible for the Divisions interactions with data, including data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction).
- Proactively supports and represents their Division with respect to matters involving data, including:
 - Appropriate use of the data within the division (in accordance with policy and legal requirements)
 - Acting as an escalation point for reporting and resolving data issues and questions
 - Representing the interests of their Divisions at the GO Committee and liaising with other members of the Committee to review and assess common/shared data issues
 - Managing and being accountable for enterprise and division-specific data governance project portfolio
 - Developing implementation plans for the data governance model within their division to address priorities set by IM Governance Committee
 - Report on progress against action plans
- Communication of data governance decisions out to their Divisions, as appropriate.

Skills and Knowledge

- Problem solving complex data interactions including risk and value impact analysis and prioritization.
- Ability to liaise with technical staff and translate technological data circumstance to business terms.
- Good understanding of data lifecycle and usage within their division, including processes for data origination, processing and controls.

Measurements

- Attendance and participation in GO Team meetings as reflected in the minutes and communications.
- On time completion of data governance portfolio projects
- Number of data issues for their division that have been analyzed and resolved.
- Satisfaction of division stakeholders being represented measured through quarterly survey and data community testimonials.
- Data governance score card with defined performance metrics for the division.

Division-specific requirements

PPH Data Environment

Population and Public Health Division (PPH) System Inventory Model			
	Collection	Use	Disclosure

s. 15

Last updated: 18-Jan-2013

Key characteristics of the environment

- Data environment:
 - Reliance on PID for some analytics and data extraction activities
 - Majority of information stored locally is aggregate (to be confirmed)
 - There do not appear to be any significant, locally-managed data sets (to be confirmed)

Considerations for governance model implementation

- The Division requires representation at the GO Committee to ensure:
 - PPH interests, risks and issues are identified and communicated
 - Key data-related decisions address PPH perspectives and priorities
- A Branch-level Data Officer network should be considered, but may not be required given PPH's data environment
- There does not appear to be a need for dataset stewards as there are no identified locally-managed datasets (to be confirmed)

Training

Training requirements

- Training will be targeted at DDOs to ensure a consistent level of understanding regarding Data Governance and relevant roles and responsibilities
- Feedback is being sought from all DDOs regarding training requirements and key topics to include

Key next steps

Next steps

- Confirm Divisional data governance “team members” based on Divisional requirements
- Delivery of training
- Transition to GO Committee (from ED Working Group)
- Initial focus on Phase 2 project oversight and support
- Working with GO Committee, identify high-priority issues and decisions that require Committee review (and escalation where required)
- Work with PID team to support implementation and ongoing operation of the governance model and related controls

Deloitte.

Divisional Data Officer Role

Pharmaceutical Services Division



September 4, 2013

Agenda

- Review DDO responsibilities
- Discuss PSD-specific considerations for governance model
- Discuss training requirements
- Next steps

Divisional Data Officer Responsibilities

Data Officers

Mandate

Responsible for a Division's interactions with data, including data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction).

Expectation of Role

- This role would require a significant investment of time from a senior staff person with a detailed understanding of division operations and management of data.
- Time required to fulfill obligations of role will vary by Division depending on amount of data administered and complexity of data use.
- Although the Data Officer would have overall accountability for data governance, they may delegate data governance activities to other team members, as needed

Data Officer – Job Description

Responsibilities

- Responsible for the Divisions interactions with data, including data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction).
- Proactively supports and represents their Division with respect to matters involving data, including:
 - Appropriate use of the data within the division (in accordance with policy and legal requirements)
 - Acting as an escalation point for reporting and resolving data issues and questions
 - Representing the interests of their Divisions at the GO Committee and liaising with other members of the Committee to review and assess common/shared data issues
 - Managing and being accountable for enterprise and division-specific data governance project portfolio
 - Developing implementation plans for the data governance model within their division to address priorities set by IM Governance Committee
 - Report on progress against action plans
- Communication of data governance decisions out to their Divisions, as appropriate.

Skills and Knowledge

- Problem solving complex data interactions including risk and value impact analysis and prioritization.
- Ability to liaise with technical staff and translate technological data circumstance to business terms.
- Good understanding of data lifecycle and usage within their division, including processes for data origination, processing and controls.

Measurements

- Attendance and participation in GO Team meetings as reflected in the minutes and communications.
- On time completion of data governance portfolio projects
- Number of data issues for their division that have been analyzed and resolved.
- Satisfaction of division stakeholders being represented measured through quarterly survey and data community testimonials.
- Data governance score card with defined performance metrics for the division.

Division-specific requirements

PSD Data Environment

Pharmaceutical Services Division (PSD) System Inventory Model Business Management, Supplier Relations and Systems (BMSRS)			
	Collection	Use	Disclosure

s. 15

Last updated: 18-Jan-2013

PSD Data Environment (2)

Pharmaceutical Services Division (PSD) System Inventory Model Drug Intelligence (DI)		
Collection	Use	Disclosure
<p>s. 15</p>		

Last updated: 18-Jan-2013

PSD Data Environment (3)

Pharmaceutical Services Division (PSD) System Inventory Model
Policy Outcomes, Evaluation and Research - Policy and Communication Programs (POER – PCP)

Collection	Use	Disclosure
------------	-----	------------

s. 15

Last updated: 18-Jan-2013

PSD Data Environment (4)

Pharmaceutical Services Division (PSD) System Inventory Model
Drug Use Optimization (DUO)

Collection

Use

Disclosure

s. 15

Last updated: 18-Jan-2013

PSD Data Environment (5)

Pharmaceutical Services Division (PSD) System Inventory Model		
Policy Outcomes, Evaluation and Research - Economist Program (POER-Econ)		
Collection	Use	Disclosure

s. 15

Last updated: 18-Jan-2013

Key characteristics of the environment

- Data environment:
 - Complex data environment with numerous incoming data feeds, local data sets and outgoing data feeds
 - Significant amount of PI used and stored across multiple branches
 - Advanced analytics and data management capabilities involving significant amounts of PI
 - Some significant datasets managed locally

Considerations for governance model implementation

- The Division requires strong representation at the GO Committee to ensure:
 - PSD interests, risks and issues are identified and communicated
 - Key data-related decisions address PSD perspectives and priorities
- A Branch-level Data Officer network will likely be required to support the DDO
- There may be a need for dataset stewards to ensure access to locally-managed datasets is appropriately coordinated

Training

Training requirements

- Training will be targeted at DDOs to ensure a consistent level of understanding regarding Data Governance and relevant roles and responsibilities
- Feedback is being sought from all DDOs regarding training requirements and key topics to include

Key next steps

Next steps

- Confirm Divisional data governance “team members” based on Divisional requirements
- Delivery of training
- Transition to GO Committee (from ED Working Group)
- Initial focus on Phase 2 project oversight and support
- Working with GO Committee, identify high-priority issues and decisions that require Committee review (and escalation where required)
- Work with PSD team to support implementation and ongoing operation of the governance model and related controls

Deloitte.

B.C. Ministry of Health Data Officer Onboarding Session

October 30, 2013
DRAFT for discussion



Agenda

Topic	Presenter	Time
Welcome & meeting objectives	Kelly Moran	5 minutes
Legislative landscape	Heather Dunlop	10 minutes
Data governance framework	Jamie Ross/Shirley Wong	20 minutes
IMG Committee Terms of Reference	Jamie Ross/Shirley Wong	20 minutes
Supporting processes	Jamie Ross/Shirley Wong	10 minutes
Key DO responsibilities <ul style="list-style-type: none"> – Point of contact regarding key policies and guidance – Information flow model maintenance – Information sharing arrangements (incoming and outgoing) – Governance Operations Committee responsibilities – Compliance – Special projects 	Heather Dunlop Melissa Murdock Kelly Moran Shirley Wong Jamie Ross	45 minutes
Questions	All	20 minutes

Meeting objectives

Meeting objectives

- The objective of this onboarding session is to ensure all Data Officers have a common understanding of the Data Officer role
- It also provides an introduction to key policies, processes and Data Officer responsibilities. This includes an overview of:
 - Relevant legislation (pertaining to health information)
 - The data governance framework and associated processes and roles and responsibilities
 - Relevant policies and guidelines
 - Who to contact with data governance, security, privacy or legislation-related questions
 - A selection of key Data Officer responsibilities
- Finally, the session provides an opportunity to connect the Data Officers with key individuals from IMKS and HIPSL who can support you in your role

Legislative landscape

The legislative landscape

- The BC health sector has a ‘patchwork’ of legislation covering the collection, use and disclosure of personal information
- As a Data Officer it is important to have a basic understanding of relevant enabling legislation, relevant privacy legislation and related guidelines
- In many cases, multiple Acts or Regulations may apply to your Division and interpretation may be difficult
- The Health Information Privacy, Security and Legislation branch (HIPSL) is available to assist in your understanding of the interplay of the various pieces of legislation (HealthInformationPrivacy@gov.bc.ca)

Additional legislation applicable to the Ministry

- There are approximately thirty (30) pieces of legislation specific to the Ministry of Health
- These include
 - enabling legislation that supports the delivery of the Ministry's mandate, and
 - Legislation which may contain additional restrictions or allowances on how personal information can be collected used and/or disclosed; key pieces of legislation include:

E.g. In an emergency situation, this Act enables designated health officers to collect, use and/or disclose personal information that under normal circumstances they would not be allowed to be collected, used and/or disclosed.

Health Professions Act

Medicare Protection Act

Pharmaceutical Services Act

Vital Statistics Act

Ministry of Health Act

E-Health Act

Public Health Act

Hospital Insurance Act

Health Professions Act

E.g. Both Acts explicitly prohibit the use of market research on the personal health information governed under these acts, despite the fact that FoIPPA makes no explicit prohibitions on market research.

BC's privacy legislation

- More generally, where a Division collects, uses and/or discloses information, it must do so in compliance with the following legislation:

Freedom of Information and Protection of Privacy Act

FoIPPA governs public bodies, including the Ministry of Health, health authorities, and many other health bodies.

The purpose of this Act is to:

- 1) Make public bodies more accountable to the public by giving the public a right of access to records as well as giving individuals the right of access to and correction of personal information about themselves; and
- 2) To protect personal privacy by preventing the unauthorized collection, use or disclosure of personal information by public bodies

Personal Information Protection Act

PIPA governs private bodies, such as physicians' offices and private laboratories.

The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Data Governance framework

“Data Governance” defined

Why is Data Governance important?

- When implemented correctly across the Ministry, data governance will have the following benefits:
 - Clarification around accountability, roles and responsibilities for data
 - Improved decision making framework that ensures that decisions are made at the right level in a prioritized and risk-based manner
 - Improved efficiency and productivity through standard and repeatable business processes
 - Enable achievement strategic and operational objectives through timely access to data
 - Reduce risk by ensuring data is adequately and consistently protected

Ministry definition:

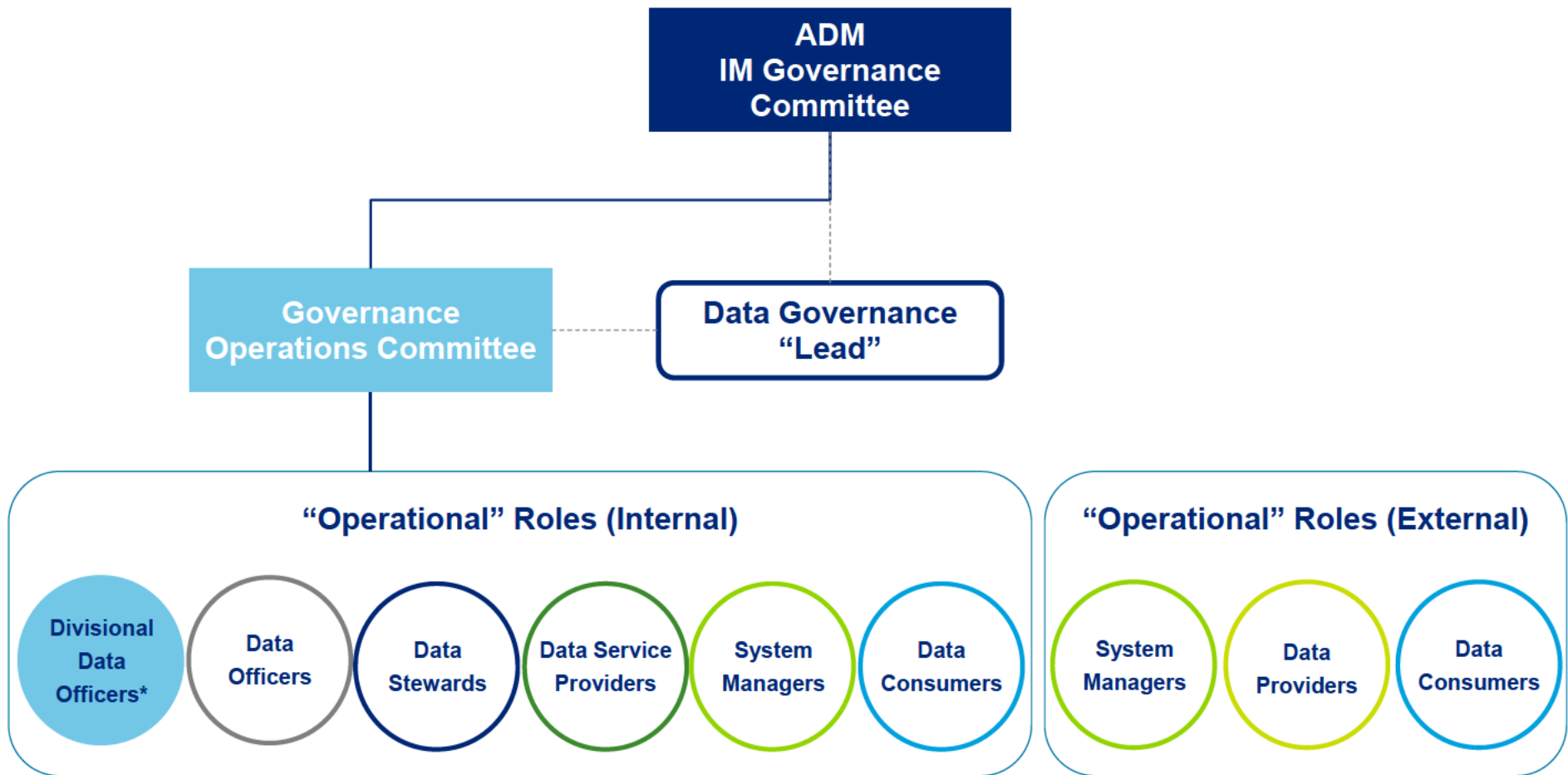
“Data governance” is the framework that promotes roles, responsibilities, processes, standards and policies to ensure the consistent and transparent management, maintenance, and utilization of Ministry data while mitigating risk.

Data governance “principles”

The Data Governance principles listed below establish the objectives for the Ministry’s Data Governance Framework and will serve to guide decisions and requirements established to operationalize the framework:

Principle 1	The Ministry values and respects data as an asset
Principle 2	Individuals understand their accountabilities for data
Principle 3	The Ministry collects, uses and discloses data for purposes consistent with its mandate and as authorized under applicable legislation
Principle 4	Authorized users can access data in support of the operational and strategic objectives of the Ministry
Principle 5	Decisions concerning data use and disclosure are made and prioritized at the appropriate level based on a transparent, consistent and risk-based decision-making process
Principle 6	The Ministry uses and discloses data in the least identifiable format possible to accomplish the intended purpose
Principle 7	The Ministry creates an adaptive, transparent and collaborative environment to support effective information management.
Principle 8	Data quality and consistent processes support timely and effective decision making and reporting

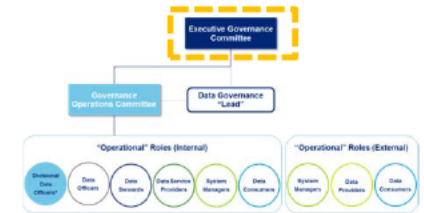
Ministry's Governance model



* Governance Operations Committee will be composed of Data Officers

Ministry's Governance model

ADM IM Governance Committee

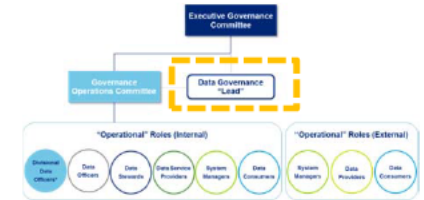


- The Information Management Governance Committee (IMG Committee) is comprised of ADMs from each Division and is responsible for overseeing, endorsing and deciding on various aspects of corporate data governance for the Ministry of Health (additional information regarding the IMG Committee Terms of Reference is provided below)
- The IMG Governance Committee is accountable for operationalizing the Ministry's data governance principles through the following activities:
 - Defining the **strategy for data governance**
 - **Prioritization and resource allocation for initiatives** related to data management
 - **Endorsement of data management policies** (including those related to data terminology, quality, protection, technology and management)
 - **Ensuring compliance mechanisms are in place** to monitor and verify adherence to data management policies and regulatory requirements

“Information management” refers to the collection, use, disclosure, retention, destruction, protection, quality and availability of Ministry data.

Ministry's Governance model

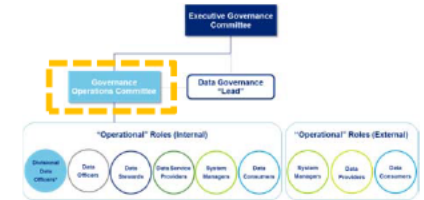
Data Governance Lead



- Data Governance Lead will be appointed by and accountable to the Health Sector IM/IT (HSIMT) ADM
- The Data Governance lead will be the **single person accountable for the implementation and operation of data governance**
- The Data Governance Lead will **support decision making within the IM Governance Committee and GO Committee**, as well as the execution of their respective mandates
- The scope of the Data Governance Lead's responsibilities may be amended from time to time by the IMG Committee

Ministry's Governance model

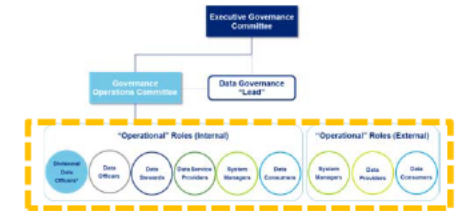
Governance Operations Committee



- Members of the IMG Committee are responsible for identifying a senior level staff member to serve as their Data Officer
- DO's will:
 1. Represent the Division's interests in relation to data management and governance and
 2. Serve as the accountable party for ensuring that data governance requirements, including principles, policies and standards, are operationalized within their Division
- Although the DO would have overall accountability for data governance within a Division, s/he may delegate data governance activities to other team members, as needed
- DOs will collaborate through the Governance Operations (GO) Committee
- The IMG Committee will assign tasks to a DO(s) through the GO Committee, in order to operationalize the Data Governance Framework and address governance-related priorities

Ministry's Governance model

Operational roles



- Data governance operational roles allow for the identification of data governance related responsibilities by types of roles that exist across the information lifecycle (**Note:** individuals may have multiple data governance roles that they function in at any point in time)
- The following table provides a high-level overview of the Ministry's data governance operational roles:

Role	Description
Data Officers	<ul style="list-style-type: none"> • Individuals responsible for the management and oversight of data handling and management within an individual division
Data Officers (delegated)	<ul style="list-style-type: none"> • Individuals appointed by the Divisional Data Office to support that individual in fulfilling the DG mandate for the division
Data stewards	<ul style="list-style-type: none"> • Individuals accountable for the management of data or data products (i.e. linked data set), including data repositories (e.g. database), data stores (e.g. LAN), and data files
Data Service Providers	<ul style="list-style-type: none"> • Individuals who extract information from systems and provide it to data consumers (whether internal or external to the Ministry)
System Managers	<ul style="list-style-type: none"> • Individuals who manage the Ministry's systems and technology infrastructure.
Data Consumers	<ul style="list-style-type: none"> • Individuals who are the end users of data and can be either internal or external to the Ministry.

IM Governance Committee Terms of Reference

IM Governance Committee TOR

- The Information Management (IM) Governance Committee Terms of Reference (TOR) serves as the basis for the DG Framework
- It incorporates components of the former IMGCC Terms of Reference, Data Stewardship Terms of Reference and other leading practices for Data Governance Terms of Reference
- Endorsement of the IM Governance Committee TOR serves as the formal basis for the Data Governance Framework, empowering the Governance Operations Committee to start its work, and create the Data Governance Lead role

IM Governance Committee TOR addresses the following:

- | | |
|--|---|
| — Purpose | — Decision making protocols (i.e. Quorum, Voting and Escalation triggers) |
| — Scope and responsibilities | — Meeting logistics |
| — Membership (unchanged) | — Deliverables and supporting documentation |
| — Supporting structures (including the Data Governance Lead and Governance Operations Committee) | — Reporting protocol |

IM Governance Committee TOR

Purpose

- The IM Governance Committee is a senior team of Ministry representatives responsible for overseeing, endorsing and deciding on various aspects of data governance
- The IM Governance Committee's is accountable for operationalizing the Ministry's data governance principles (see Appendix A – Data governance principles) through the following activities:
 - Defining the **strategy for data governance**
 - **Prioritization and resource allocation for initiatives** related to data management
 - **Endorsement of data management policies** (including those related to data terminology, quality, protection, technology and management)
 - **Ensuring compliance mechanisms are in place** to monitor and verify adherence to data management policies and regulatory requirements

“Information management” refers to the collection, use, disclosure, retention, destruction, protection, quality and availability of Ministry data.

IM Governance Committee TOR

Scope and responsibilities

- The IM Governance Committee has overall responsibility and accountability for Ministry data
- Its objective is to provide oversight and set direction on roles, responsibilities, processes, standards and policies as well as ensure consistent and transparent management, maintenance and utilization of Ministry data while mitigating risk
- The extent to which the IMGc's mandate will include analytics will be determined following completion of the analytics strategy
- Areas of specific focus under this mandate include:



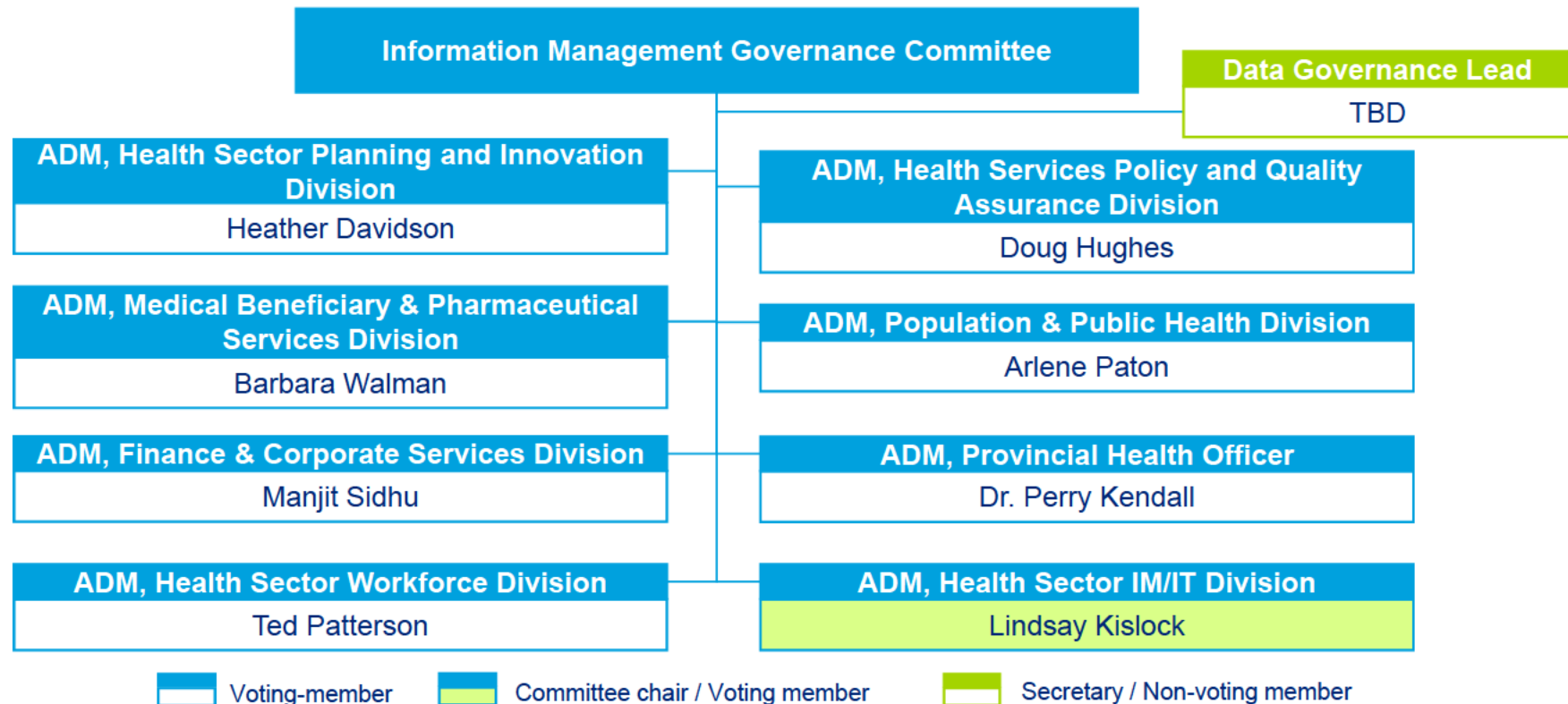
The IM Governance Committee:

- ✓ Responsible for setting Ministry direction and strategy in relation to IM and data governance, including the provision of strategic direction in relation to utilizing Ministry data as a corporate asset (with respect to risk mitigation and business enablement)
- ✓ Defines data governance strategic priorities
- ✓ Establishes, endorses and reviews the Ministry's data governance policies and standards
- ✓ Is accountable for the Ministry's overall compliance with IM policy and legislation
- ✓ Manages and approves the Ministry's investment in data assets that impact multiple Divisions
- ✓ Allocates Data Officer resources to the Governance Operations (GO) Committee and to data-related initiatives on a priority basis
- ✓ Provides direction to GO Committee and Data Officers, as required
- ✓ Serves as the final decision-making body for escalated data governance issues and decisions
- ✓ Establishes KPIs for measuring and reporting on the management of and compliance with the Data Governance Framework

IM Governance Committee TOR

Membership

- The Committee is comprised of the most senior representatives of the Business and IM functions (ADMs) with authority to act on behalf of their respective divisions
- The Data Governance Lead will serve as the secretary for the Committee as well as participate in the Committee as a non-voting member



IM Governance Committee TOR

Supporting structures

Data Governance Lead

- Data Governance Lead will be appointed by and accountable to the Health Sector IM/IT (HSIMT) ADM
- The Data Governance lead will be the **single person accountable for the implementation and operation of data governance**
- The Data Governance Lead will **support decision making within the IM Governance Committee and GO Committee**, as well as the execution of their respective mandates
- The scope of Data Governance Lead's responsibilities may be amended from time to time by the IMGC
- See Appendix B – Data Governance Lead Job Description

The scope of responsibilities of the Data Governance Lead includes:

- ✓ Supporting the effective implementation of the Data Governance Framework;
- ✓ Supporting the development of governance policy, standards and processes and ensuring alignment with corporate and/or government policies, standards and processes;
- ✓ Managing all aspects of day-to-day data governance activities including communications, measurement and reporting;
- ✓ Reviewing and advising on Executive decisions for data governance initiatives;
- ✓ Managing the GO Committee project portfolio, the data services help desk and serving as the secretary to the IMG Committee and the GO Committee; and
- ✓ Supporting operational reporting on data governance metrics.

IM Governance Committee TOR

Supporting structures (cont.)

Governance Operations (GO) Committee

- Members of the IM Governance Committee are responsible for identifying a senior level staff member to serve as their Divisional Data Officer
- Data Officers will be accountable for their Division's interactions with data; including, data issues and decisions in relation to terminology, standards, quality, protection, and lifecycle management (creation through destruction)
- Divisional Data Officers will represent the Division's interests in relation to data management and governance and serve as the accountable party for ensuring that data governance requirements, including principles, policies and standards, are operationalized within their Division (see Appendix C – Data Officer Job Description)
- Although the Data Officer would have overall accountability for data governance within a Division, s/he may delegate data governance activities to other team members, referred to as Data Officers, as needed
- Divisional Data Officers will collaborate through the Governance Operations (GO) Committee
- The IM Governance Committee will assign tasks to a Data Officer(s) through the GO Committee, in order to operationalize the Data Governance Framework and address governance-related priorities

IM Governance Committee TOR

Supporting structures (cont.)

Governance Operations (GO) Committee

The IMG Committee can delegate the following types of data-related decisions and activities to the GO Committee:

- ✓ Representing the data interests of respective Divisions in the delivery of the Ministry's strategic and operational objectives
- ✓ Defining, prioritizing and operationalizing a portfolio of data-related projects that address strategic priorities set by the IMG Committee
- ✓ Raising and resolving key operational data issues and decisions in relation to data terminology, quality, protection, technology and management
- ✓ Providing recommendations to the IMG Committee on responsibilities, processes, standards and policies in relation to Ministry data as well as key data governance issues, risks and decisions;
- ✓ Providing periodic reporting on the project portfolio
- ✓ Escalating risks/decisions to the IMG Committee
- ✓ Supporting IMG Committee decision-making on escalated issues by preparing decision support material and presenting to the Committee as required
- ✓ Periodic reporting to the IMG Committee that addresses data-related KPIs (i.e. quality, training, project progress, DSAs, etc.)

IM Governance Committee TOR

Other structures set out in TOR

- Additional structures set out in the IM Governance TOR include:
 - **Decision-making protocol:** provides an overview of how decisions will be made by Committee; including,
 - Quorum,
 - Decision/voting, and
 - Escalation
 - **Deliverables and supporting materials:** describes responsibilities with respect to creating, distributing and maintaining materials
 - Strategic plan,
 - Decision support materials,
 - Meeting minutes, and
 - Issue/Decision log
 - **Reporting protocol:** provides the responsibility and frequency for which Committee activities will be reported

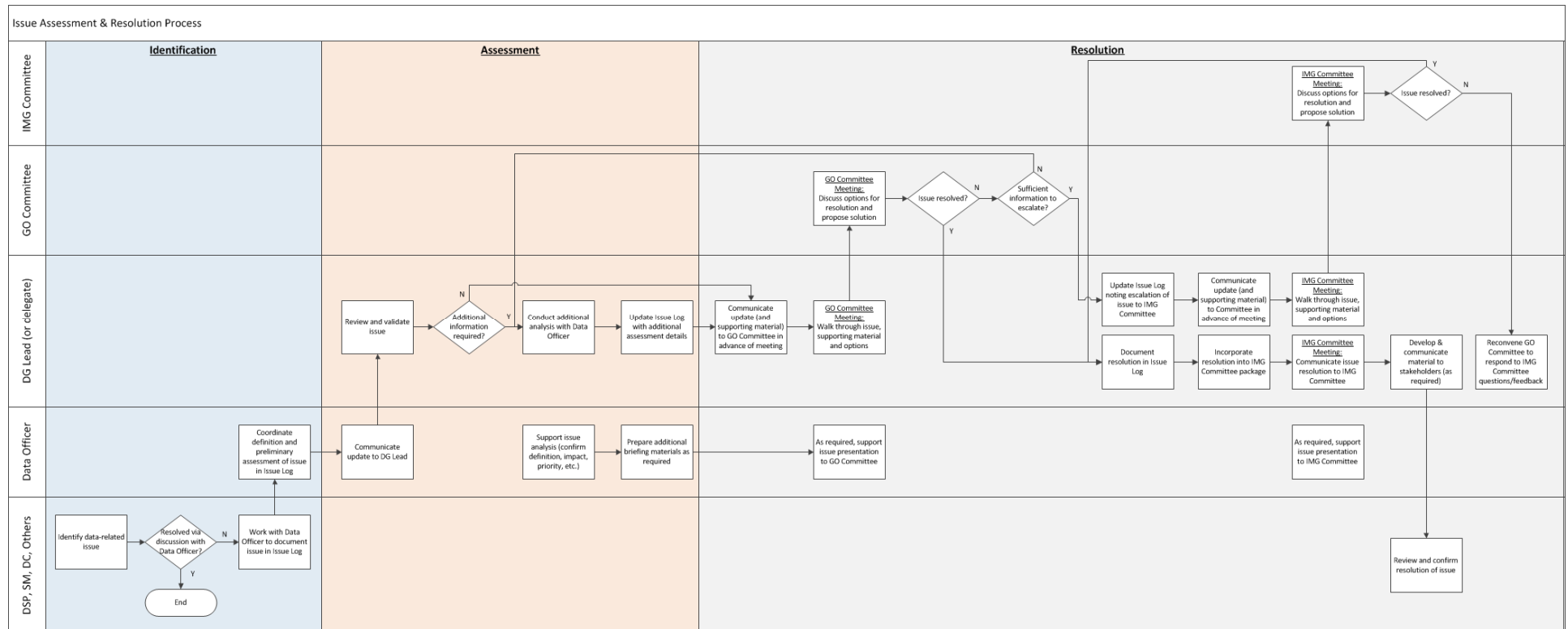
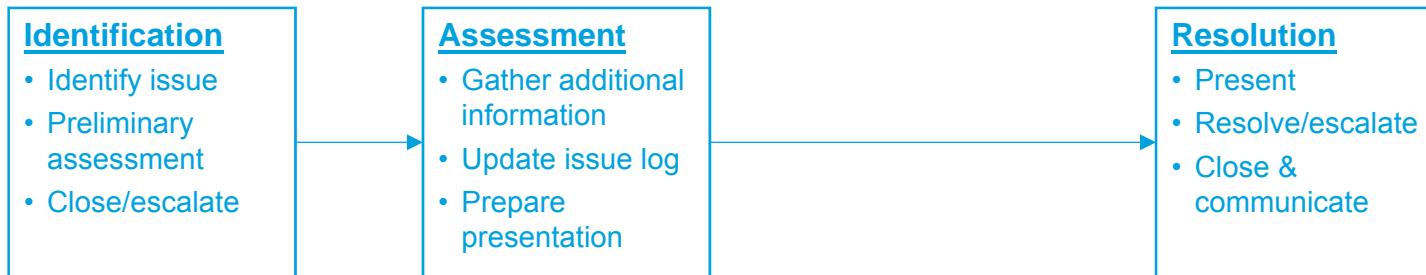
Supporting processes

Supporting data governance processes

Issues assessment process

- The purpose of this process is to provide a mechanism for data-related issues to be:
 - Identified
 - consistently documented
 - assessed
 - resolved or escalated as required
- Three key steps:
 - **Identification** - issues can be identified and raised by anyone (end user, business owner, IT representative, etc.). They should be reported to the Data Officer for evaluation and potential resolution.
 - **Assessment** – if the issue cannot be resolved, the DO will document the issue in an issue log and escalate to the office of the Data Governance Lead
 - **Resolution** - once assessed and documented, the issue will be raised to the Governance Operations Committee for resolution. If resolution is not possible, the issue is escalated to the IM Governance Committee as needed

Issue Assessment Process



Key DO responsibilities

Overview of select Data Officer activities

- Point of contact regarding key policies and guidance
- Information flow model maintenance
- Information sharing arrangements (incoming and outgoing)
- Governance Operations Committee responsibilities
- Compliance
- Special projects

Relevant policies & guidelines

Relevant policies and guidelines

- The OCIO, IMKS and HIPSL have developed information security and management policies and guidelines applicable to the Ministry
- Key Ministry policies and guidelines are listed in the table below for your reference; as a DO you are responsible for familiarizing yourself with these policies and their application to your Division
- HIPSL is available to assist you in interpreting the requirements in these policies, as needed (HealthInformationPrivacy@gov.bc.ca)

Policy / guideline	Description	Additional support
Core Policy and Procedures Manual	Chapter 12: Information Management and Information Technology Management, provides guidance for key legislation (e.g. FIPPA); define authorities, responsibilities and accountabilities for information and technology management; and provides an overview of the government's policy framework and operational activities required for the management of information and technology activities. http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm	IMKS
FOIPPA Policy and Procedures Manual	This manual breaks down and provides guidance on FOIPPA, including providing a high-level summary, policy, procedure and interpretation for each section within the Act. http://www.cio.gov.bc.ca/cio/priv_leg/manual/index.page	HIPSL

Relevant policies and guidelines (cont.)

Policy / guideline	Description	Additional support
Information Security Policy	<p>This policy provides the framework for government organizations to establish local policies and procedures necessary for the protection of information and technology assets for the Province of British Columbia. http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf</p>	
	<p>The Policy Summaries provide guidance on how the ISP applies to a subject area with regards to government personnel (i.e. all employees as well as other individuals such as contractors, volunteers and third-party organizations) and managers. While all summaries are important for Data officers to read and understand, the following require particular attention:</p> <ul style="list-style-type: none"> ▪ No. 1 – Overview of ISP ▪ No. 3 – Portable Storage Devices ▪ No. 8 – Encryption ▪ No. 9 – Information Security Events and Incidents ▪ No. 11 – Logging and Monitoring ▪ No. 12 – Security Awareness ▪ No. 16 – Protection of Sensitive Information ▪ No. 19 – Information Sharing and Exchange Agreements ▪ No. 26 – Access Control Management ▪ No. 32 – Information Security Classification <p>http://www.cio.gov.bc.ca/cio/informationsecurity/policy/isp_summaries.page</p>	HIPSL

Relevant policies and guidelines (cont.)

Policy / guideline	Description	Additional support
Information Incident Management Process	This policy provides direction for employees and business owners (including supervisors and service providers) in responding to incidents that threaten information privacy or security. http://www.cio.gov.bc.ca/cio/information_incident/index.page	HIPSL
The General Health Information Sharing Agreement (GHISA)	Provides an overarching framework (including roles and responsibilities, governance and related terms) for the sharing of information with Health Authorities.	IMKS
Guidelines for Best Practices in Data Management – Roles and Responsibilities	This document provides guidance on the data management model described in Chapter 12 of the CPPM and how to build and improve this capability. http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/data_mgt_roles_responsibilities_guidelines.pdf	IMKS
Data Set Access	Data access processes for internal Ministry parties	IMKS

Information flow models

Information flow model

What is an information flow model?

- Information flow models are a graphical representation of the flow of data within each of the Ministry's Divisions. Specifically, they include:
 - The source of information that is collected by each Division, the level of aggregation of the data (i.e. personal information or aggregate information) and the mechanism (e.g. e-mail, paper, etc.) by which the data is transmitted
 - The systems, databases and applications that are used to manage, handle, share and store the data
 - The stakeholders, including those internal and external to the Ministry, with whom the data is shared, and the mechanism by which sharing takes place
- *Note: these models are based on the system inventories submitted by key representatives from each Division in December, 2012*

Information flow model

Why are the information flow models important?

- The models provide a baseline understanding of information handling activities within each of the Ministry's divisions, by identifying the following:
 - Branches and/or teams that handle health-related information
 - Major information sources used by those branches or teams
 - Movement of information within the Ministry and between the Ministry and external parties
 - Methods of information transmission
 - Major information storage locations
- This baseline supports a risk-based approach to prioritizing information management and protection activities by providing answers to some key questions:
 - Where do we collect sensitive information from?
 - Where is this information stored?
 - How do we manage sensitive information? What controls are in place?
 - Who do we provide sensitive information to? Are agreements in place? Is the sharing of this information necessary?

Maintenance of information flow models

- Maintaining an updated information flow model is critical to understanding the risks related to sensitive information in each Division
- It is recommended that these models be maintained and updated on a regular basis (note: each Division may customize their model as they see fit)
- In Divisions with complex data holdings and flows, the Data Officer may delegate this task to one or more Branches as appropriate
- It is recommended that the first task involve a review and update to these models to reflect:
 - Recent organizational changes
 - Technical changes to each Division's environment over the past 12 months

Information sharing agreements

Information sharing agreements – incoming data

- If your Division is evaluating the acquisition of data from a third party, there are several key steps to consider prior to entering into a contractual arrangement
 - Ensure the Ministry has the legal authority to collect the information under consideration (engage HIPSL for support as required)
 - Engage IMKS to ensure there is a review of the relevant security and privacy terms in the agreement and to confirm that these terms can be met
 - Work with IMKS and HIPSL to identify and implement appropriate controls to support compliance with the terms in the agreement where necessary (e.g., access control, logical and/or physical security controls, etc.)
 - Where necessary, identify a process for monitoring compliance with contract terms

Information sharing agreements – outgoing data

- There are well-defined processes and templates related to information sharing (and many have recently been updated)
- When your Division is evaluating a new sharing arrangement with a third party, it is recommended that you use the tools defined on the Ministry's website to guide the process (<http://www.health.gov.bc.ca/data/>)

The screenshot shows the British Columbia Ministry of Health website. The header includes the British Columbia logo, a search bar, and links for Advanced Search, Contact Us, and Text Size. Below the header is a navigation bar with links for News, The Premier Online, Ministries & Organizations, Job Opportunities, and Main Index. The left sidebar contains a 'B.C. Home' section with links to Ministry of Health, Health Data Central, Academic Researchers, Health Authorities, Health Data Request Forms, Other Organizations, and Web Application Services. Below this is a 'GOVERNMENT' section with links to Quick access to information based on government's structure, B.C. Government, Ministries and Organizations, and Other Levels of Government. The main content area features a large banner for the Ministry of Health and a section titled 'Health Data Central' with a welcome message and a list of data access request types: Academic research requests for Ministry of Health data, Health authority program evaluations and public health surveillance, and The creation of information sharing agreements with other organizations. A 'TOP' link is located at the bottom right of the main content area.

[COPYRIGHT](#) | [DISCLAIMER](#) | [PRIVACY](#) | [ACCESSIBILITY](#)

Governance Operations Committee

Governance Operations Committee responsibilities

- As a DO you are responsible for the proactive representation of your Division via the GO Committee, including the following activities:
 - Escalating Divisional data-related issues, opportunities, risks and decisions to the GO Committee, as needed
 - Liaising with other members of the GO Committee to review and assess common/shared data issues and opportunities
 - Seeking input from Subject Matter Experts within your Division regarding key data issues or opportunities
 - Recommending actions to be taken to resolve issues or advance opportunities
 - Participating in the decision-making process for data-related issues and opportunities
 - Inform or be a direct participant in work projects with respect to data domains
 - Report on progress against action plans

Compliance

Compliance activities

- The Ministry will be establishing a compliance monitoring function to support alignment with Ministry and Government requirements
- Data Officers will be a point of contact for each Division on compliance-related activities
- Initially, this will involve tracking of progress of initiatives that are currently underway (and that align with commitments made to external bodies)
- Over time, this approach will support sharing of lessons learned and best practices related to information management and protection

Special projects

Special projects

- The focus of the Data Officers in the short term will be on select Ministry-wide projects that are underway or planned
- The purpose of this approach is to ensure cross-Ministry engagement and transparent decision-making for these key initiatives, and to provide an opportunity to evaluate and adjust the governance model as required
- Key initiatives include:
 - Condor Transition and SAS Upgrade (currently underway)
 - Secure Access Environment (planned)
 - OIPC Progress Reporting

Questions?

Deloitte.

From: Gannon, Sean R HLTH:EX
To: Dunlop, Heather L HLTH:EX; Townson, Martin HLTH:EX; Stodola, Gordon M HLTH:EX; Madden, Ken HLTH:EX; Gregory, Tom HLTH:EX; Hayward, Ross HLTH:EX; Higgs, Jeremy HLTH:EX; Voggenreiter, Christine HLTH:EX; Wong, Shirley M HLTH:EX; Brar, Dave S HLTH:EX; Bryant, Soji HLTH:EX; Fairbotham, David J HLTH:EX; Gray, David HLTH:EX; Jennings, Suzanne VSA:EX; Liu, Meiying HLTH:EX; Pennock, Mike HLTH:EX; Smith, Stephen H HLTH:EX; Spearman, Mark VSA:EX; West, Randi HLTH:EX; Wong, Mei HLTH:EX; Yang, William HLTH:EX; Reimer, Kim HLTH:EX; Ford, Dave G HLTH:EX; Jepp, Tim HLTH:EX
Cc: Pourmalek, Saloumeh HLTH:EX; Witcher, Rob (CA - British Columbia); Minvielle, Catherine M HLTH:EX
Subject: RE: Data Management projects - Phase 2 - Project 2.1.a LAN access removals
Date: Tuesday, August 13, 2013 6:37:37 PM
Attachments: [image001.png](#)
[FW HAD LAN Permissions Review - HAD LAN Decommissioning Request Project 2.1 .msg](#)
[FW Project 2.1 delete accounts from HAD Lan folders - Complete.msg](#)

All,

Per message below, picking up where things left off with you in April/May 2013 on the LAN clean-up work.
Per below, I am facilitating this work on behalf of Catherine Minvielle and Kelly Moran.

Scope for this Phase:

Removing “red” users, i.e. people who are no longer in your Division (or possibly even the Ministry) from having access to your LAN by September 30th, 2013.


The “New Ask” at this time:

1. **By August 23, 2013:** Send a LAN decommissioning and/or LAN access change request email to hlth.helpdesk@gov.bc.ca
Subject line “(your branch or Division name) LAN project 2.1”,
 - include a covering instruction such as “delete the people highlighted red, they no longer work in my Division.”
 - See attached mock example based on the submission Soji did for HAD (now HPS Division).
Within approx. 1-3 weeks you will get a note back from Helpdesk (or Denise and Keith in Authentication Services) saying this request is complete (see second attachment)
2. You will email the confirmation to myself Sean.Gannon@gov.bc.ca and cc Catherine.Minvielle@gov.bc.ca in advance of September 30th.

Thanks.

Background Notes:

What *should* have happened already:

1. You or your delegate(s) for your Divisions would have been asked to send Stephen Braniff a list of LAN’s your staff use. For example I sent him a note and told him HealthLinkBC branch (one of the eight HSIMIT branches) is on 
2. Mike Botrakoff (CMO-HSIMIT) or Stephen Braniff would have sent you back a note a few weeks later saying “see attached list of current access for your area, please submit any access changes to the helpdesk”.
 - (If either of these steps have not happened please email myself and Catherine indicated what has not yet occurred)

If you already have this confirmation and you are done, GREAT, please send your confirmation note to Sean and Catherine per above.

If your area is doing a more complete LAN review (Great!) and that work has scope beyond the September 30th deadline, happy to report out on the Maturity of steps taken in your area as part of the Management report out on this deliverable,

- With the proviso that you meet the minimum ask of removing the red users for your Division by September 30th.

Please consider the turnaround time Helpdesk needs, and endeavor to have your (remove red user) “LAN project 2.1” email to hlth.helpdesk@gov.bc.ca by August 23rd or sooner, to allow clarification or for more resources to be added if helpdesk is swamped.

Please forward this to a delegate if you have delegated this work in your area or if several branch leads are involved. If this is the case, please email Catherine and Sean the delegate names so we know who we need to work with directly.

For those I have not had a chance to chat with in person yet, please feel free to contact me directly with questions on this. I will be out of office August 14-23 inclusive but will have limited access to email over that time, otherwise I will be following up with you when I return on August 26th.

Thanks in advance,

From: Minvielle, Catherine M HLTH:EX
Sent: Friday, August 9, 2013 9:45 AM
To: 'Melissa Cielen'; Gannon, Sean R HLBC:EX; Braniff, Stephen HLTH:EX; Dunlop, Heather L HLTH:EX; Townson, Martin HLTH:EX; Stodola, Gordon M HLTH:EX; Drouin, Denis HLTH:EX; Madden, Ken HLTH:EX; Bell, Carolyn P HLTH:EX; Gregory, Tom HLTH:EX; Hayward, Ross HLTH:EX; Higgs, Jeremy HLTH:EX; Minvielle, Catherine M HLTH:EX; Moran, Kelly P HLTH:EX; Perri, Maria A HLTH:EX; Voggenreiter, Christine HLTH:EX; Wong, Shirley M HLTH:EX; Brar, Dave S HLTH:EX; Bryant, Soji HLTH:EX; Fairbotham, David J HLTH:EX; Gannon, Sean R HLBC:EX; Gray, David HLTH:EX; Jennings, Suzanne VSA:EX; Liu, Meiyong HLTH:EX; Pennock, Mike HLTH:EX; Smith, Stephen H HLTH:EX; Spearman, Mark VSA:EX; West, Randi HLTH:EX; Wong, Mei HLTH:EX; Yang, William HLTH:EX
Cc: Moran, Kelly P HLTH:EX; Pourmalek, Saloumeh HLTH:EX; Wong, Shirley M HLTH:EX; Ross, Jamie HLTH:EX; 'MacPherson, Don (CA - Alberta)'; XT:Yap, Albert CITZ:IN; 'Rob Witcher'
Subject: Data Management projects - Phase 2

Good morning,

Thank you for all your contributions to the success of phase 1 Data Management and Security Projects. We successfully completed our objectives in large part to the efforts you made, and positioned the Ministry to respond well to the recent Information and Privacy Commissioner report. We are now progressing on the "phase 2" projects, and the project management team has been working hard to put together project charters and work plans for these projects over the past few weeks. Once again, we are requesting your engagement and insight to represent your division's interests and coordinate your division's participation in the delivery of these Ministry-wide projects.

Over the next week to ten days we will be sending you invitations to seek your assistance with the following projects:

Project Name + Objective	Project Lead	Activities + Timelines	
2.1 a – LAN Clean up	Sean Gannon	Implementation of LAN access changes (Aug 16 – Sep 16)	
2.1 b – Enhancement Opportunities	Sean Gannon	Agreement on approach and implementation of enhancement opportunities (Aug 1 – Sep 16)	
3.x – Condor Transition	Stephen Braniff (IMKS) Mei Wong (PID)	New data warehouse, web application environment, and SAS analytics	
		Business Managers Working Group (Aug – Dec 2013)	<ul style="list-style-type: none"> Ensure research officer resources are made available Communicate status update and issues to executive Agreement and input on project Charter
		Research Officer Working Group (Aug – Dec 2013)	<ul style="list-style-type: none"> Ensure timely migration of business data and user acceptance testing Provide information regarding raw data usage Communication of staff roles & responsibilities within their divisions with a focus on information access & sharing. Provide input regarding key priorities and approaches for training
6.3 – Information Sharing Agreements	Melissa Murdock	New Information Sharing Agreements for 10 priority/high risk areas of information sharing situations that do not have any agreements in place currently (Sep 6 – Sep 30)	

Over the next couple of weeks we will provide a comprehensive overview on the projects and the governance model changes, and we will gauge interest in a presentation/discussion on the "big picture" of phase 2 work; if there is sufficient interest the project team will be happy to walk through the current status.

If you have questions, please contact myself or in my absence Catherine Minvielle who continues as project manager for this work, or Saloumeh Pourmalek who is coordinating our communications for this next phase. Thanks very much.

Kelly

Confidentiality Warning: This message and any attachments are intended only for the use of the intended recipient(s), are confidential, and may be privileged. If you are not the intended recipient, you are hereby notified that any review, retransmission, conversion to hard copy, copying, circulation or other use of this message and any attachments is strictly prohibited. If you are not the intended recipient, please notify the sender immediately by return e-mail, and delete this message and any attachments from your system.

Information confidentielle: Le présent message, ainsi que tout fichier qui y est joint, est envoyé à l'intention exclusive de son ou de ses destinataires; il est de nature confidentielle et peut constituer une information privilégiée. Nous avertissons toute personne autre que le destinataire prévu que tout examen, réacheminement, impression, copie, distribution ou autre utilisation de ce message et de tout fichier qui y est joint est strictement interdit. Si vous n'êtes pas le destinataire prévu, veuillez en aviser immédiatement l'expéditeur par retour de courriel et supprimer ce message et tout document joint de votre système. Merci.

From: [Gannon, Sean R HLBC:EX](#)
To: [Gannon, Sean R HLBC:EX](#)
Subject: FW: HAD LAN Permissions Review - HAD LAN Decommissioning Request Project 2.1
Date: Tuesday, August 13, 2013 5:53:22 PM
Attachments: [Mock Example - HAD decommissioning request.xlsx](#)

From: Bryant, Soji HLTH:EX
Sent: Thursday, July 18, 2013 10:53 AM
To: Minvielle, Catherine M HLTH:EX
Subject: FW: HAD LAN Permissions Review

Soji

Soji Bryant, MBA.

Director, Planning and Division Operations

Phone: (250) 952-2175 BB: (250) 516-4361 Fax: (250) 952-1052

From: Will, Jordan HLTH:EX
Sent: Thursday, July 4, 2013 3:44 PM
To: Helpdesk, HLTH HLTH:EX
Cc: Braniff, Stephen HLTH:EX; Bryant, Soji HLTH:EX
Subject: HAD LAN Permissions Review

Hi,

Please find the attached spreadsheet for LAN Permissions in HAD, s. 15 Could you please remove the specified folder permissions of those people listed in **RED**.

If you have any questions or concerns, please let me know.

Thank you

JORDAN WILL

A/Policy and Planning Analyst

Health Authorities Division

Phone: (250) 952-1867

	A	B	C	D	E	F	G
1	Group Name	Members	Full Name	Company	Department	Title	Email
2	s. 15	Mmouse	Mickey Mouse	Health	Physician Compensation - MSHHRD	Senior Manager	Mickey.Mouse@gov.bc.ca
3		Mmouse	Mickey Mouse	Health	Physician Compensation - MSHHRD	Senior Manager	Mickey.Mouse@gov.bc.ca
4		Mmouse	Mickey Mouse	Health	Physician Compensation - MSHHRD	Senior Manager	Mickey.Mouse@gov.bc.ca
5		Mmouse	Mickey Mouse	Health	Physician Compensation - MSHHRD	Senior Manager	Mickey.Mouse@gov.bc.ca
6		ACURR	Alana Currentstaff	Health	Patient Safety and Care Quality	ED Admin Assistant	Mickey.Mouse@gov.bc.ca
7		ACURR	Alana Currentstaff	Health	Patient Safety and Care Quality	ED Admin Assistant	Alana.Currentstaff@gov.bc.ca
8		ACURR	Alana Currentstaff	Health	Patient Safety and Care Quality	ED Admin Assistant	Alana.Currentstaff@gov.bc.ca
9		ACURR	Alana Currentstaff	Health	Patient Safety and Care Quality	ED Admin Assistant	Alana.Currentstaff@gov.bc.ca
10		ACURR	Alana Currentstaff	Health	Patient Safety and Care Quality	ED Admin Assistant	Alana.Currentstaff@gov.bc.ca
11		ACURR	Alana Currentstaff	Health	Patient Safety and Care Quality	ED Admin Assistant	Alana.Currentstaff@gov.bc.ca
12		AALSOCU	Allie AlsoCurrentStaff	Health	Healthy Minds, Healthy People Directorate, HAD	Project Manager, Healthy Minds, Healthy People Directorate	Allie.Alsocurrentstaff@gov.bc.ca
13		AALSOCU	Allie AlsoCurrentStaff	Health	Healthy Minds, Healthy People Directorate, HAD	Project Manager, Healthy Minds, Healthy People Directorate	Allie.Alsocurrentstaff@gov.bc.ca
14		AALSOCU	Allie AlsoCurrentStaff	Health	Healthy Minds, Healthy People Directorate, HAD	Project Manager, Healthy Minds, Healthy People Directorate	Allie.Alsocurrentstaff@gov.bc.ca
15		AALSOCU	Allie AlsoCurrentStaff	Health	Healthy Minds, Healthy People Directorate, HAD	Project Manager, Healthy Minds, Healthy People Directorate	Allie.Alsocurrentstaff@gov.bc.ca
16		DDUCK	Donald Duck	Health	Research, Knowledge Translation and Library Services Branch, Pla	Policy Analyst	Donald.Duck@gov.bc.ca
17		DDUCK	Donald Duck	Health	Research, Knowledge Translation and Library Services Branch, Pla	Policy Analyst	Donald.Duck@gov.bc.ca
18		DDUCK	Donald Duck	Health	Research, Knowledge Translation and Library Services Branch, Pla	Policy Analyst	Donald.Duck@gov.bc.ca
19		DDUCK	Donald Duck	Health	Research, Knowledge Translation and Library Services Branch, Pla	Policy Analyst	Donald.Duck@gov.bc.ca
20		MIMOUSE	Minnie Mouse	Health	Organizational Development & Engagement	Coordinator	Minnie.Mouse@gov.bc.ca
21		MIMOUSE	Minnie Mouse	Health	Organizational Development & Engagement	Coordinator	Minnie.Mouse@gov.bc.ca
22		MIMOUSE	Minnie Mouse	Health	Organizational Development & Engagement	Coordinator	Minnie.Mouse@gov.bc.ca

	A	B	C	D	E	F	G
23	s. 15	MIMOUSE	Minnie Mouse	Health	Organizational Development & Engagement	Internal Communications Coordinator	Minnie.Mouse@gov.bc.ca
24		MIMOUSE	Minnie Mouse	Health	Organizational Development & Engagement	Internal Communications Coordinator	Minnie.Mouse@gov.bc.ca
25		MIMOUSE	Minnie Mouse	Health	Organizational Development & Engagement	Internal Communications Coordinator	Minnie.Mouse@gov.bc.ca
26		MIMOUSE	Minnie Mouse	Health	Organizational Development & Engagement	Internal Communications Coordinator	Minnie.Mouse@gov.bc.ca
27		ASTILLC	Angela Stillcurrent	Health	Health Authority Relations and Corporate Services	Manager, Health Authority Relations	Angela.Stillcurrent@gov.bc.ca
28		ASTILLC	Angela Stillcurrent	Health	Health Authority Relations and Corporate Services	Manager, Health Authority Relations	Angela.Stillcurrent@gov.bc.ca
29		ASTILLC	Angela Stillcurrent	Health	Health Authority Relations and Corporate Services	Manager, Health Authority Relations	Angela.Stillcurrent@gov.bc.ca
30		ASTILLC	Angela Stillcurrent	Health	Health Authority Relations and Corporate Services	Manager, Health Authority Relations	Angela.Stillcurrent@gov.bc.ca
31		AFHERES	Angela F Herestill	Health	Patient Care Quality Review Board - HAD	Intake Officer	Angela.F.Herestill@patientcarequalityreviewboard.ca
32		AFHERES	Angela F Herestill	Health	Patient Care Quality Review Board - HAD	Intake Officer	Angela.F.Herestill@patientcarequalityreviewboard.ca
33		AFHERES	Angela F Herestill	Health	Patient Care Quality Review Board - HAD	Intake Officer	Angela.F.Herestill@patientcarequalityreviewboard.ca
34		AFHERES	Angela F Herestill	Health	Patient Care Quality Review Board - HAD	Intake Officer	Angela.F.Herestill@patientcarequalityreviewboard.ca
35		AFHERES	Angela F Herestill	Health	Patient Care Quality Review Board - HAD	Intake Officer	Angela.F.Herestill@patientcarequalityreviewboard.ca

From: [Gannon, Sean R HLBC:EX](#)
To: [Gannon, Sean R HLBC:EX](#)
Subject: FW: Project 2.1 delete accounts from HAD Lan folders - Complete
Date: Tuesday, August 13, 2013 5:54:46 PM

From: Rempel, Denise HLTH:EX
Sent: Tuesday, August 13, 2013 10:34 AM
To: Will, Jordan HLTH:EX; Gannon, Sean R HLBC:EX; Bryant, Soji HLTH:EX
Cc: hlth Authentication Services; Townson, Martin HLTH:EX; Minvielle, Catherine M HLTH:EX; Wall, Beryl E HLTH:EX
Subject: Project 2.1 delete accounts from HAD Lan folders - Complete

This request has now been completed as requested

From: Rempel, Denise HLTH:EX
Sent: Thursday, August 08, 2013 03:17 PM Pacific Standard Time
To: Helpdesk, HLTH HLTH:EX
Cc: hlth Authentication Services; Gannon, Sean R HLBC:EX; Will, Jordan HLTH:EX; Bryant, Soji HLTH:EX; Townson, Martin HLTH:EX; Wall, Beryl E HLTH:EX; Minvielle, Catherine M HLTH:EX
Subject: FW: Good morning

Helpdesk : please log a cam call under Project 2.1 for this request to delete accounts from HAD Lan folders

We can submit the istore to have this actioned and will advise

Denise Rempel
Technical Analyst, Security Administration
Information Management and Knowledge Services
Health Sector IM/IT Division
Ministry of Health
2-1 1515 Blanshard St
Victoria, BC V8W 3C8
250 952-2490 (Phone)
250 952-1119 (Fax)

Note: This message is confidential and may not be disclosed to anyone without the express written consent of the sender.

From: Gannon, Sean R HLBC:EX
Sent: Thursday, August 8, 2013 2:53 PM
To: Rempel, Denise HLTH:EX
Cc: Helpdesk, HLTH HLTH:EX; Townson, Martin HLTH:EX; Minvielle, Catherine M HLTH:EX
Subject: FW: Good morning

FYI Denise,

This is the other one I mentioned that I wasn't sure if it has made it to you
I think Catherine already chatted with Martin on this 'request to remove the red ones' ☺

If this is the first time you are seeing it, "here you go, let me know if there are issues"

Just got off the phone with Jordan and he mentioned he had met with Keith before his vacation but Jordan did not seem to know where things were at now, or if more was required from him
If there is a value add I can do with Soji or Will Jordan let me know

Ps Catherine, Martin FYI only

/SG

	A	B	C	D	E	F
1	2.1.a Branch/Div	Contact	Status	date sent to helpdesk or ETA	# of LANs submitted / total number of LANs	Helpdesk Completion date
2	HAD	Soji Bryant, Jordan Will	Complete	aug 08 2013		aug 13 2013
3	PID	Dave Brar, Dave Ford, Tim Jepp	Aug 28/30 submitted 14 lists total	Aug 28/30 submitted 14 lists total		Auth Serv -in progress ETA mid Nov due to many restore access issues associated with the early submissions
4	FCS	Stephen Smith	09 03 Plan B will address the highest risk LAN folders and the plan is to be complete by 30 September. Review process is well underway and the plan is to have lists submitted by week of 16-20 September.	Consolidated list emailed 12 September	all	Complete - Denise email 10-08
5	PPH/PHO	Kim Reimer	<p>09 04 Persons no longer with the Ministry have been identified (100% complete). Persons no longer with PPH/PHO but still with the Ministry - identifying which specific PPH/PHO drives no longer needed (75% complete). Persons with PPH/PHO - identifying non-essential drives as a result of changing roles within PPH/PHO (75% complete).</p> <p>From: Gannon, Sean R HLBC:EX Sent: Friday, September 27, 2013 5:28 PM So if I am reading this right, You have emailed all the green sheets to helpdesk already, And the only server lists you have left to do are these three s. 15 yes?</p> <p>From: Vander Kuyl, Wendy HLTH:EX Sent: Monday, September 30, 2013 11:59 AM I sent the file to the Helpdesk this morning. I think I'm down to the last 4 or 5 people now – so will bug them individually.</p> <p>s. 15 ? already included in my spreadsheets</p> <p>s. 15 no PPH employees listed</p> <p>s. 15 ? already included in my spreadsheets</p> <p>s. 15 no deletions for PPH/PHO, so no green tab</p> <p>25% completed, on target (Catherine connected with Jeremy on Sept 03.)</p> <p>All branches have the relevant LAN access lists. September 20th is given as the due date for submitting the requests for deletion. I will continue to follow-up until the end of the month.</p> <p>From: Higgs, Jeremy HLTH:EX Sent: Wednesday, September 25, 2013 9:01 AM I'm still hearing back from all the branches. We've had some additional completions in the Lab/Diagnostics/Blood area, Medical Services Commission and Medical Services Branch. Still waiting to hear back from Physician Compensation and few of the smaller areas. I have not had time to personally bug anybody but will get on people tomorrow in person.</p>	09 04 Will submit non-Ministry by Sept 6. Will submit non-PPH/PHO by Sept 13. Will submit non-essential drive information as available aiming to complete by Sept 20.	Oct 04 Sean sent Wendy PPH a note to confirm it is indeed 100% done.	Auth Serv -in progress ETA Mid Nov due to many restore access issues associated with the early submissions
6	MSD	Jeremy Higgs	Submitted (Aug) also completing some preexisting project work/routine maintainance on s. 15 as PSD is moving to consolidate the Divison onto s. 15	One list was sent September 3, 2013 (Negotiations Support)	Oct 04 Sean sent Jeremy a note for final confirm it is indeed 100% done.	Completed Oct 15
7	PSD	Christine Voggenreiter/Charlotte Elagab	Submitted (Aug) also completing some preexisting project work/routine maintainance on s. 15 as PSD is moving to consolidate the Divison onto s. 15	2013-08-01 s. 15 and the one other drive done 09		Completed Oct 15
8	HSIMIT CMO	Don Stewart, Andrew Elderfield	<p>Email from Don May 21 asking Stephen how to format the submission fo s. 15</p> <p>May 23 note: developing ORCS, and ETA for LAN changes end of Sept. Needs Update</p> <p>Janet emal 09-03 on track for end of sept</p> <p>From: Hastings, Bonny HLTH:EX</p> <p>Sent: Tuesday, October 1, 2013 8:48 AM To: Helpdesk, HLTH HLTH:EX</p> <p>Cc: Gannon, Sean R HLBC:EX; Lucas, Janet HLTH:EX</p> <p>We have reviewed the LAN Access for the BMO LAN and I have attached a spreadsheet with the red highlighted names can be removed from having access to our</p> <p>s. 15</p>	06		completed Sep 5 2013
9	HSIMIT BMO	Janet Lucas	s. 15	Complete	all	Complete
10	HSIMIT SPB	Leila Ball	<p>From: Ball, Leila Sent: 19, 2013 3:50 PM To: Helpdesk, HLTH HLTH:EX Hi again, apologies that this first pass didn't work for removing access. I've completed the review of the associated groups and included them in the attached spreadsheets. In it you will find a tab for each share, the group names and the people/IDs from our branch (SPB) that can be removed from those groups. Hopefully that will provide the info you need to clean up the access for those people in our branch.</p>	Sept 19 second pass	all	Completed Oct 15
11	HSIMIT HITS	June Allin	Complete	(August)		s.15
12	HSIMIT HLBC	Sean Gannon	Submitted July 30th	Submitted July 30th		Completed Sept 11 2013
13	HSIMIT VSA	Suzanne Jennings	09/11 email from Suzanne Jennings: A review has been performed and all Users who are no longer VSA staff or contracted resources have had their access to the VSA LAN removed.	Complete		Complete
14	HSIMIT IMKS	Shirley Wong, Stephen Braniff, Brandie Frawley	From: Frawley, Brandie HLTH:EX Sent: Monday, September 23, 2013 4:21 PM To: Gannon, Sean R HLBC:EX I have completed 3 of the 8 tabs to be reviewed. There are 5 tabs to review by the September 30th deadline.	Don Rintoul submitted	all 8	Due to high volume of opearational requests, this 2.1 Project is not anticipated to be actioned until at least November
15	HSIMIT HIPSL	Deb McGinnis	May 17 note: identified clean up opportunities on s. 15 needs update no status on "red users.	Chris Reimer sent request to decomission s. 15		Completed SEP -6-2013

	A	B	C	D	E	F	G	H
1	Phase 2 Project 2.1b Enhancement Opportunity Status Updates Oct 30, 2013							
2								
3								
4	2.1.b Branch/Div	Contact	Status	Denis has list of names for mtg invites? Room booked yes no	Date Material Prepared or ETA	Date Meeting(s) held (or to be held)	Meeting Outcome (management)	Committment Date
5	HAD	Soji Bryant, Jordan Will	Kick off meeting week of Sept 02-06, agreement on out of scope items, agreement on communications/education/one pager approach, Div agreed to provide list of names for next meeting, Denis to set up mtg(s) asap.	<p>Oct 17 - email communication with Danielle Prpich (A/ED). November 19/13 is earlier can meet with HIPSL. Rob W has affirmed this date.</p> <p>Oct 15 - Catherine, Sean & Denis spoke with ??? To request a meeting with key staff for the EO review.</p> <p>* Communicated with ED and A/ED requesting a date to meet with HIPSL</p> <p>* Discussed concerns with Soji's response. Catherine and Rob discuss Soji's response with Kelly M.</p> <p>Oct 01 Soji response - As I mentioned previously, we are currently working through a reorganization that is still not yet fully determined. I am aware that you need to have this set up, however I am still not prepared to respond regarding a time and date that will work for us. I will let you know once we are in a position to go ahead with the work session.</p> <p>Sept 13 Soji response - Soji indicated that the changes are fairly significant in their area – they have a new ADM starting next week and are anticipating that the final structure will not be confirmed for at least two weeks. They are not ready to set a time or send out invitations.</p>	HIPSL will use existing materials already developed and made available to Ministry staff.	Completed Oct 30/13	October 30 - 20 minute meeting - Delivered discussion with HSD (formerly HAD) covering their EO's. As they are commencing on changes to their business and work space, they may request HIPSL to conduct a site visit to assist with EO changes.	Soji Bryant Oct 30/13
6	FCS	Stephen Smith	Kick off meeting week of Sept 02-06, agreement on out of scope items, agreement on communications/education/one pager approach, Div agreed to provide list of names for next meeting, Denis to set up mtg(s) asap.	Janice Saxby & Rita King are set for a work session Sept 21st.		Completed Sept 21/13	<p>Your workplace information security practices are very good, as you have</p> <ul style="list-style-type: none"> - Locked storage cabinets (locked at all times) that do not have markings to indicate the contents. Audit binders are locked in cabinets/desks when not in use. Binders are not signed in/out as you are aware of who has them (e.g., a small team of auditors and a pharmacists). - The work area is clean and tidy; staff immediately shred documents using the area's central locked shred bin. Staff use the common recycle (blue) bin for non-sensitive materials. - Staff lock sensitive materials in desks/cabinets when the materials are not in use/staff leave their desks. - All audit staff/pharmacists and admin staff have keys to cabinets. - Your multifunction device (MFD) is only used by staff – staff do not need to send locked printouts to the device, as they immediately pickup documents. - Rarely staff may need to access the worksite to store materials when returning from an audit. Normally, staff do not have 24 hour access to the building. If they need temporary, after-hours access, they can submit a ministry form to request temporary access. From facilities, you can obtain a list of your staff who have accessed the building after-hours, as a periodic review. - Staff are advised to not leave sensitive materials unattended in their car/home when working away from the office. - You use ministry meeting rooms for staff meetings. <p>You share a common wall with non-ministry government communications staff (the top portion of the wall is open as per heating, ventilation, and air conditioning (HVAC) requirements – it would be quite expensive to add a complete wall and comply with HVAC requirements). During our site visit (11:30-noon), it was quiet and we could not hear neighbouring conversations from the communications staff or others east of your worksite (past pillar B2).</p>	Ted Boomer Oct 07/13

	A	B	C	D	E	F	G	H
4	2.1.b Branch/Div	Contact	Status	Denis has list of names for mtg invites? Room booked yes no	Date Material Prepared or ETA	Date Meeting(s) held (or to be held)	Meeting Outcome (management)	Committment Date
7	MSD	Jeremy Higgs & John English	Kick off meeting week of Sept 02-06, agreement on out of scope items, agreement on communications/education/one pager approach, Div agreed to provide list of names for next meeting, Denis to set up mtg(s) asap.	Working with Sharlene Drewniak and with Christine Hume and Monica Marcos from Physician Compensation Branch to set a meeting date/time/location.		Completed Oct 04/13	Oct 17 - emailed a followup communication to the Directors and support staff in Adopted solutions - not certain if this program area has implemented any of the proposed changes.	Jeremy Higgs & John English Oct 17/13
8	PSD	Christine Voggenreiter/Charlotte Elagab	Kick off meeting week of Sept 02-06, agreement on out of scope items, agreement on communications/education/one pager approach, Div agreed to provide list of names for next meeting, Denis to set up mtg(s) asap.	<p>Oct 17 - emailed Christine Voggenreiter/Charlotte Elagab requesting assistance in determining date, time and key staff for a meeting with HIPSL. Tentative date is October 23/13.</p> <p>Oct 15 - left a message with Christine Voggenreiter to request a meeting with key staff.</p> <p>Oct 10 sent email to Derek - requesting update to dates/times.</p> <p>Oct 01 response- Derek has had difficulty finding rooms. He believes we may have to do 3-4 sessions. He will contact in the next week with an update.</p> <p>Derek Tryan (for Christine/Charlotte). Branch meeting in Victoria.</p> <ul style="list-style-type: none"> * Policy group * New West - 25 people (likely a 'Live Meeting' session) - travel restrictions * Victoria - 80 people - October 2 & 7 		Completed Oct 23/13	<p>October 23 - meeting outcome:</p> <p>This past summer, the division has discussed the Deloitte items and how the division could implement enhanced information protection practices. Several staff have had past information privacy and security presentations, yet there has been a lot of change (reorganization and new staff).</p> <ol style="list-style-type: none"> 1. Need more confidential shred bins – how do we obtain them? 2. Where is the 1 ministry media bin? (for CDs, etc). Answer: It is in the bin labelled 'Recall for Media Disposal' the 1515 Blanshard mailroom (see the secure disposal bulletin below). 3. There needs to be increased signage over shred bins (e.g., 'shred bin'). 4. There needs to be more signage/stickers to warn about locking materials (e.g., perhaps stickers 'before leaving, lock your files!') or discussing sensitive conversations, particularly in open areas/elevators (e.g., "sensitive conversations should not be discussed here'). Setting the appropriate culture is a huge (yet important) task that needs to be ongoing. 5. Staff are aware of picking up printouts yet sometimes, in a hurry this is not done. Staff notice printouts on the printer and deliver to the intended recipient (so they are being vigilant). What more can be done? The team will discuss ways to manage printing and ask HIPSL for advice/guidance as required. Answer: Staff can lock printouts so that you must unlock the print jobs at the printer (see the document link in the next section). The government is leaning towards having locked printouts with the upcoming multi-function device refresh. 	Oct 23 - possible follow up meeting
9							6. The division is doing branch plans, would this be an opportunity to ask HIPSL to attend to give a presentation on a topic? What about branch/unit meetings?	
10							Answer: Yes, absolutely to both. If you have a specific topic, please send it to Gwen	
11								
12							7. It is often hard to know how to classify information, such as prior to an item being	
13							Answer: Information has a lifetimes – often it is sensitive prior to release and then may become public after. The government has a high-level classification framework that is to be used to classify all information. The ministry is working on adapting this framework to develop relevant practices in the ministry. In particular, looking at the harm that could occur (to individuals, organizations, financial or reputational harm). HIPSL is looking to divisions to provide us with case studies so that a ministry-specific framework and guidance criteria can be used.	
14								
15							The division would be receptive to an informal walk through to look at opportunities	

MOH P MOH Phase 2: Project 2.1.b. Rationalize enhancement opportunities identified by Divisions (to inform Phase 2 priorities)

6 Security Principle	Division Response	Enhancement Opportunity	Source Division	Information Source Document	Project Mapping
<p>1. Sensitive and personally identifiable data:</p> <p>a. Must be classified according to the government's information security classification framework.</p> <p>b. Must only be shared with individuals who have a "need to know" and only to the level required ("least privilege") for the least amount of time.</p> <p>c. Must be encrypted to government standards if the data is moved to a portable storage device (including yet not limited to a laptop, notebook/tablet, CD, portable hard drive, Smartphone, or government encrypted USB memory stick)</p> <p>d. Must not be transmitted by fax unless it is absolutely necessary to transmit the information, and speed of transmission is essential (e.g., when there are time-critical circumstances affecting health or safety, or when it is</p> <p>e. Should remain on secure government storage internally in the ministry.</p>	<p>- The majority of HAD's work falls in the Medium Classification (with the exception of Treasury Board/Cabinet Submission documents). Correspondence contains personal information and is stored on LAN. Identified Remediation Opportunity: move correspondence to a secure drive.</p>	Correspondence containing personal identifiable information restricted to a secure drive	Health Authorities Division	"HAD - 6 Security Principles Document.docx"	
	<p>- The MSHHRD does not formally do this on a case by case basis. To our knowledge, MSHHRD does not do this as yet. The MSHHRD operates on a principle that all work is carried out on a 'need to know' basis. Summary data is provided to MSHHRD staff an estimated 85% of the time with the remaining extracts and analyses limited to core functions such as enforcing billing rules and service contracts.</p>	<i>Need to clarify with MSD</i>	Medical Services Division	"MSD from email.docx"	
	<p>- Conversations about confidential topics -- for example, with drug manufacturers or stakeholders -- could be overheard by people not in PSD</p>	Staff education about discussing confidential information in secure environments e.g. meeting rooms to prevent unauthorized information sharing	Pharmaceutical Services Division	"PSD - List of Identified Opportunities - V2.xlsx"	Projects 4.1 + 4.2
	<p>- PI data resides on Condor under specific restricted paths.</p> <p>- Datasets for the predictive modeling are stored on Condor</p>	PI data storage limited to secure environments with access management controls	Planning & Innovation Division	"PID - Goal 1 PID Division Summary (v3).xlsx"	Projects 2.2 + 3.2
	<p>- Regular concerns about security role proliferation and maintenance costs:</p> <p>i) Using the least privilege model, we have the potential to end up with multiple variations of the same role, all requiring maintenance</p> <p>ii) The more security roles we have the less likely DSAM will be able to keep track of them, and tell 'at a glance' what access a User has, resulting in a less comprehensible and less secure environment.</p>	Clearly defined roles based access management system implementation	HealthLink BC / HSMIT / Vital Statistics	"HSIMT - IMKS - email.docx"	Projects 5.x
	<p>- Disposal of information when it is no longer needed. Admittedly, this will be a challenge as we are intensive users of data. Those of us accessing data tend to move from project to project so we don't take/have time to clean-up as we go. One opportunity is to keep the extraction and analysis programs but delete anything else that won't be needed.</p>	Disposal of information no longer needed. Staff education on Information Disposal policy, standards, and procedures	Medical Services Division	"MSD from email.docx"	Project 2.1
	<p>- Billing Integrity Program – deleting data files downloaded from MSP onto Condor after use by audit staff. Provide existing contractors an overview of MOH's security requirement and for future contracts the security requirement will be included in their orientation.</p>	<i>Same as above</i>	Financial and Corporate Services Division	"FCSD - email.docx"	Projects 2.1 + 2.2 + 3.2
	<p>- HAD is working with IMIT to take a risk management approach given the broad nature of our sensitive work. Until this is completed, HAD is unable to be fully compliant.</p>	Restricted use of unencrypted portable storage devices	Health Authorities Division	"HAD - 6 Security Principles Document.docx"	
	<p>- Very limited use of fax for transmission of sensitive or personal data in HAD</p>	- Restricted use of fax for transmission of sensitive or personal data in HAD	Health Authorities Division	"HAD - 6 Security Principles Document.docx"	Project 4.2
	<p>- The MSHHRD never transmits information by fax but occasionally received information by fax from practitioners and patients.</p>	<i>Same as above</i>	Medical Services Division	"MSD from email.docx"	

6 Security Principle	Division Response	Enhancement Opportunity	Source Division	Information Source Document	Project Mapping	
2.	Individuals handling the sensitive and personally identifiable data must secure it when it is not being used (e.g., clean work space; store in locked file cabinets) and prior to being securely destroyed according to government standards.	- Confidential documents are left on desks or chairs when people are away from their cubicles - Confidential documents are stored below desks or in cubicle recycle bins - Confidential documents are printed and left on or near the printer - Confidential presentation materials are distributed to attendees without procedures for disposal - Confidential documents, including unencrypted CD roms containing archived SA requests, are stored in file cabinets in the unsecured area in the branch, some of which are unlocked	Staff education on Information Storage policy, standards and procedures to promote use of locked cabinets for storing confidential documents	Pharmaceutical Services Division	"PSD - List of Identified Opportunities - V2.xlsx"	Projects 4.1 + 4.2 + 9.1
		- On occasion, documents with sensitive/personal information left on desk e.g., briefing notes, cabinet submissions. Identified Remediation Opportunity: Ensure staff are aware to use locked filed cabinets or desk drawers for sensitive and personally identifiable information, even if they have locked offices.	Same as above	Health Authorities Division	"HAD - 6 Security Principles Document.docx"	Projects 4.1 + 4.2 + 9.1
		- Some employees take work home. Identified Remediation Opportunity: Staff are encouraged to store items on LAN and access remotely, or access information from laptop where data is encrypted on hard drive.	Staff education on Working from Home policy, standards and procedures to promote use of encrypted devices and remote LAN access	Health Authorities Division	"HAD - 6 Security Principles Document.docx"	
		- The MSHHRD has an opportunity to improve the after-hours secure storage of some paper records containing practitioner numbers while a project is underway. - PharmaCare Audit – consider logging files in and out of existing locked cabinets	Same as above Use of logging and checking system for accessing documents from locked cabinets	Medical Services Division Financial and Corporate Services Division	"MSD from email.docx" "FCSD - email.docx"	
3.	Using good workplace security practices, such as locking workstations/laptops when you leave them, as described i the ministry's <u>Information and Workplace Security Guide</u> .	§ 15 - Printing reports with sensitive/personal information when printouts go to a common room. Identified Remediation Opportunity: Staff are made aware of the need to lock print jobs when printing sensitive or personal information to a common print room.	Replacement of key operated locks with scanner and combination locks Same as above	Pharmaceutical Services Division HealthLink BC / HSMIT / Vital Statistics Health Authorities Division	"PSD - List of Identified Opportunities - V2.xlsx" "Heal hlink - email.docx" "HAD - 6 Security Principles Document.docx"	 Projects 4.1 + 4.2 + 9.1
4.	Ensuring that appropriate accountabilities, agreements, assessments (including, yet not limited to information sharing and confidentiality agreements, privacy impact assessments and security, threat, and risk assessments) and documented data handling practices (including security awareness training) are used before accessing the sensitive and personally identifiable data or using it in collaboration tools (e.g., SharePoint and LiveMeeting) or outside the workplace.	- HAD is working with IMIT to take a risk management approach given the broad nature of our sensi ve work	Strict usage and periodic renewal of appropriate agreements to foster a culture of accountability	Health Authorities Division	"HAD - 6 Security Principles Document.docx"	Projects 6.x
		- Issue on interpretation of what requires an agreement when MSHHRD data use is completely tied to legislated functions such as administering physician compensation (via fee-for-service and alternative payments) and Physician Master Agreement requirements such as the Medical On Call Availability Program and the General Practice Service Committee. Again, summary data are used for the most part. – Update ICBC ISA as expires this year – process commenced; enter into an ISA wi h Canada Border Service Agency to improve information sharing	Same as above	Medical Services Division	"MSD from email.docx"	Projects 6.x
			Same as above	Financial and Corporate Services Division	"FCSD - email.docx"	Projects 6.x
5.	Periodically reviewing access to the sensitive and personally identifiable data regardless of where it is stored (e.g., on the local area network including shared and personal ("C:" or " H:" drives), laptops, removable storage, or SharePoint) and promptly removing access when it is no longer required. Unusual access patterns, or suspected/actual information incidents must be immediately escalated to management using he government's Information Incident Process.	- Confidential documents, emails, and data queries are saved on the C or H drive (including the desktop) and not deleted	Periodic access management and information usage audit across the organization and systems	Pharmaceutical Services Division	"PSD - List of Identified Opportunities - V2.xlsx"	Projects 5.4 +7.2 + 10.1
		- Some areas of MSHHRD need to improve on his. For example, the need to monitor LAN accesses and the means to do so was communicated to MSHHRD management. Further communication and progress monitoring will be undertaken.	Same as above	Medical Services Division	"MSD from email.docx"	Projects 5.4 +7.2 + 10.1
		§ 15		HealthLink BC / HSMIT / Vital Statistics	"Heal hlink - email.docx"	

6 Security Principle	Division Response	Enhancement Opportunity	Source Division	Information Source Document	Project Mapping
	- Annual review and sign off of access authoriza ions (currently reviewed periodically). This could include conducting spot audits/checks on what staff are accessing when using Ministry databases to confirm justified, and reviewing inactive accounts to determine if necessary.	Annual review and sign off of access authorizations	Financial and Corporate Services Division	"FCSD - email.docx"	
6.	Individuals being aware of their obligations, as described in the government's Standards of Conduct, Core Policy (Chapters 12, 15, and Loss Reporting), and government Information Security Policies and Standards.				

Notes:

- [Population and Public Health Division](#): Not sure if the 2 survey results listed on summary document are enhancement opportunities, as they are in compliance. Hence no opportunity identified for PPH.

Pages 210 through 211 redacted for the following reasons:

s. 15

Email Template to Data Officers for Access Review

Dear XXXX

Industry best-practices dictate that access to data sets with Personally Identifiable (PI) or sensitive data be reviewed on a regular basis. As part of the Data Set Access Management review process, you, as the Data Officer for your division, are being provided with a current list (as of DATE) of those with access to PI data within the XXX dataset. This particular dataset is reviewed on an (annual, bi-annual, quarterly) basis (list attached).

- Please review this list of users to verify that their access is appropriate, based on their role
- If you have concerns about any of those listed please contact the appropriate supervisor or Director of that individual and discuss these concerns.
- If any action to an individual's access is to be taken this is to be worked out between you and the individual's Director.
- DSAM has no role as middle-man in these discussions
- Once a decision to remove or restrict access has been made then please email DSAM, providing them with the details of the access change, including why the access is being removed or reduced. Please include a confirmation that the individual's supervisor or Director has agreed to this action.
- DSAM will inform the client that access is being removed (though the client should already have been informed by their Director).
- DSAM will inform you when the access has been removed.
- Please respond to DSAM within 2 weeks, informing them if any action is required or not. Even if there is no action to be taken DSAM needs to be notified so that a record of access reviews can be maintained for audit purposes.
- If DSAM has not received a response within the 2 weeks, we will contact you or your alternate one more time to request a response.
- If this second email is not responded to within a week we will contact your Executive Director or ADM to request a response.

Data Set Access Management

Schedule of Access Review and Monitoring Activities

1. *Audit Report*

- a. Automatically generated at the beginning of each month status on accounts not accessed for 3 months, or 12 months
- b. DSAM reviews and begins processing the same day report is received/generated

2. *Departing Employee Forms*

- a. All are dealt with each Monday morning (though many may get dealt with on the day of receipt)

3. *HR Activity Report*

- a. Received weekly (not same day each week though)
- b. Reviewed and processed within 24 hours of receipt

Page 214 redacted for the following reason:

s.15

Data Set Access

Non HSIMT managed Data sets

For Ministry of Health datasets and databases managed outside of HSIMT the role of managing access to that data is handled under the auspices of each Divisional Data Officer. To ensure the proper management of data access the following two approved policies have been developed for the Data Officer and individuals responsible for non-HSIMT managed data sets.

Policy 1: Role of the Divisional Data Officer for non-HSIMT managed data sets [*place link here*]

Policy 2: Data Access managed outside of the HSIMT Division [*place link here*]

As well, for audit purposes, a template Excel spreadsheet has been developed to capture the activities around data access management. The use of this particular template is optional, but the capturing and retention of the information is not. Therefore if a different method is used to capture the required information please be sure that it is comprehensive.

Database Access Excel template: [*place link here*]

HSIMT managed Data sets

For Ministry of Health databases, managed by HSIMT Division, role-based access is provided based on the data set and the type of identifiable information required by Ministry of Health employees and contractors.

Data Set Access Management (DSAM) provides final approval on requests to access these databases, based on authority delegated by the Ministry's Chief Data Steward. The following three criteria are used to determine access to data sets:

- The *right information* is granted (e.g. appropriate level of access)
- To the *right person* (e.g. access required to fulfill current job or project requirements)
- At the *right time* (e.g. access granted only for the duration of the requirements)

To ensure that the correct level of access is granted, a description of the job function(s) and an example of how the information will be used is required. In most cases, analysts will want access to the

s. 15

DSAM may need to provide evidence that appropriate access is being granted. Therefore, all requests, background information, access justification, etc. must be provided by email through the 7076 Database Access Request form.

DSAM routinely suspends access to data sets (i.e. locks the account) if an account is inactive for 90 days. If your account is locked and you still require access, please contact DSAM.

Accounts that have been inactive for 12 months are closed and require the submission of a new 7076 request to be re-opened.

The process

- Request arrives in Data Set Access Management (DSAM) inbox by way of a Ministry of Health DSAM Databases Access Request form (7076).
- The technical administrator (TA) verifies:
 - that the form is complete, including appropriate justification to access the requested data. If request is from a MoH Service Provider, service contract must also be provided with the request to confirm the relationship, nature of work performed and the duration of the contract
 - that the requester's supervisor has approved the request
 - that the level of access requested aligns with the purpose for requesting. TA may:
 - seek more information from the person making the request or their supervisor.
 - consult with the identified data SME to confirm access level is required as per the purpose for requesting
 - seek direction from Senior Data Warehouse Architect or Director, Data Access - for more complex requests. This particular step can take some time and is completely beyond the control of DSAM.
- Confirm appropriate database security role to assign.
- TA assigns a role based on the request.
- User account created or updated.
- TA notifies requester with access confirmation and log on credentials.

Policy for HSIMT managed Data Set Access

HSIMT Policy Directive DSAM managed – terminations [*place link here*]

HSIMT Policy Directive DSAM managed – transfers [*place link here*]

Communications Plan

Project 5.4

1. A document will be provided to the Divisional Data Officers outlining the DSAM annual review schedule for HSMIT managed datasets. The responsibility of the Data Officer will be outlined in the email template that will accompany each review.
2. Data Officers will be asked to promote the policy within their own division by informing those who may handle the reviews for them (if not done by themselves).
3. The Weekly Ministry Bulletin will be used to promote this activity to ministry staff.

Project 5.6

4. Policy documents will be provided to the Divisional Data Officers.
5. Data Officers will be asked to promote the policy within their own division by providing copies to all those who manage data
6. Once a web page home has been determined/or created, the policies will be posted to that web page. For these policies it should be an intranet page, internal facing, as this is ministry internal policy.
7. The Weekly Ministry Bulletin will be used to point ministry staff to the policy web page.
8. Intent is to have both 5.4 and 5.6 completed by the end of October.

Projects 5.4 & 5.6 Phase 2



**ACCESS REVIEW PROCESS FOR
HSIMT MANAGED DATASETS
(5.4)
NON-HSIMT MANAGED DATASET
ACCESS MANAGEMENT (5.6)**

Projects 5.4 & 5.6, Phase 2

- Both the Deloitte and OIPC reviews recommended a stronger access review process
- Data Set Access Management has created a process for access review of datasets managed by HSIMT (5.4)
- Policy has been created for the managing access of those datasets managed by other areas in the Ministry (5.6)

I'll walk through both processes for you

Projects 5.4, Phase 2

- DSAM generated access review reports will be generated on a quarterly, semi-annual, or annual basis
- All users as of the day report generated will be included
- Data officer will receive and have 2 weeks to review and reply
- DSAM must hear back from the Data Officer in order to close the review in the access review log for audit purposes

- based on activity in the database
- Complete list of all users
- The list will come with an email detailing the process
- If no response within 2 weeks another email will go out, and if no response within a week of that, then the Divisional ADM will be contacted

Projects 5.4, Phase 2



- DSAM plays no role in determining if someone is to be removed or not
- The Data Officer, in consultation with the individual's Director, will make that determination

Projects 5.4, Phase 2

s. 15 Access List Test Version

All users with access to MSP PI data

Person	E-mail Address	MSP	MSP Start
Jane Doe	jane.do@gov.bc.ca	MSP	2007-06-15
Betty Boop	betty.boop@gov.bc.ca	MSP	2012-02-13
Clark Kent	clark.kent@gov.bc.ca	MSP	2007-06-15
Lois Lane	lois.lane@gov.bc.ca	MSP	2007-10-09
Rhett Butler	rhett.butler@gov.bc.ca	MSP	2013-07-16
Scarlette O'hara	scarlette.ohara@gov.bc.ca	MSP	2007-10-09
James T Kirk	james.t.kirk@gov.bc.ca	MSP	2008-12-19
Al Capone	al.capone@gov.bc.ca	MSP	2011-11-17
Elliott Ness	elliott.ness@gov.bc.ca	MSP	2007-10-09

Sample of the report



• Questions

Projects 5.6, Phase 2



Non-HSIMT managed dataset access management

- Policy has been set to manage access to HSIMT managed datasets
- There is a need to mirror that policy for all the datasets not managed by HSIMT

Projects 5.6, Phase 2

- This policy has been drafted and is working its way through an approval process
- Once it is finalized it will be shared with the Data Officers
- One of the policies is designed for the Data Officer
- The other policy is designed for those who actually manage a dataset

The policy is basic and talks about the responsibility for keeping track of who gets access, removing access, allowing access only under the 'least privilege' and 'need to know' basis

Policies talk about 'locking' access for temporary reasons such as TAs, Maternity Leaves, etc.

Policies talk about 'terminating' access for staff moves, retirements, etc.

Projects 5.6, Phase 2



- Both policies speak to the need to maintain a complete record of access management
- This is needed for audit purposes
- We have created a simple Excel spreadsheet which we will provide to anyone who wants to use it

Projects 5.6, Phase 2



XX Database Access						
Database Data Steward: XX YY						
Name of Requestor	Name of Approver	Date Access Granted	Date Access Locked	Reason Access Locked	Date Access Terminated	Reason Access Terminated

Reason Access Locked

- 1 = on a TA outside the office
- 2 = on Maternity or Paternity leave
- 3 = STIP longer than a month
- 4 = LTD
- 5 = Deferred Salary Leave
- 6 = Leave without Pay
- 7 = temporary re-assignment of duties

Reason Access Terminated

- A = left ministry for another ministry
- B = left position
- C = Dismissed
- D = Deceased
- E = Retired
- F = LTD - not returning



• Questions?

	B	C	D	E	F	G
1	Data Access Review Schedule					
2	Data Sets with PI or Sensitive data only					
3						
4	Dataset	Division	Divisional Data Officer	Data User	Frequency	Date
5		ID	Carolyn Bell	Randi West	Annually	December
6		ID	Carolyn Bell	Randi West Stephen Braniff/Jeremy Higgs	Annually	February
7		ID	Carolyn Bell	Dave Brar	Annually	March
8		ID	Carolyn Bell	Randi West	Annually	April
9						May
10		s.15		Don Rintoul Carlos Caraveo	Annually	June
11		HAD	Ross Hayward	Robin McMillan	Annually	December
12			Don Rintoul	Don Rintoul Carlos Caraveo	Annually	August
13		SD	Maria Perri	Rita King David Fairbotham Monica Uribe David	Annually	September
14		inance	Maria Perri	Fairbotham	Annually	October

	B	C	D	E	F	G
1	Data Access Review Schedule					
2	Data Sets with PI or Sensitive data only					
3						
4	Dataset	Division	Divisional Data Officer	Data User	Frequency	Date
15	s.15	Finance	Maria Perri	Maire Thelisma	Annually	November
16		PSD	Christine Voggenreiter	David Fairbotham	Bi-Annually	January/July
17		PID	Carolyn Bell	Diane Foort	Bi-Annually	February/August
18		PID	Carolyn Bell	Dave Brar	Bi-Annually	March/September
19		PID	Carolyn Bell	Dave Brar	Quarterly	April/July/Oct/Jan
20		MSHHRD	Jeremy Higgs	Jeremy Higgs	Quarterly	May/Aug/Nov/Feb
21		PSD	Christine Voggenreiter	Christine Voggenreiter	Quarterly	June/Sept/Dec/Mar
22		HSIMT	Shirley Wong	Jack Shewchuk	Quarterly	July/Oct/Jan/April

	A	B	C	D	E	F	G
1							
2							
3	XX Database Access Database Data Steward: XX YY						
4							
5	Name of Requestor	Name of Approver	Date Access Granted	Date Access Locked	Reason Access Locked	Date Access Terminated	Reason Access Terminated
6							
7							
8							
9							
10							
11							
12							
13	Reason Access Locked		Reason Access Terminated				
14	1 = on a TA outside the office		A = left ministry for another ministry				
15	2 = on Maternity or Paternity leave		B = left position				
16	3 = STIIP longer than a month		C = Dismissed				
17	4 = LTD		D = Deceased				
18	5 = Deferred Salary Leave		E = Retired				
19	6 = Leave without Pay		F = LTD - not returning				
20	7 = temporary re-assignment of duties						

	A	B	C	D
1	s. 15 Access List Test Version			
2	All users with access to MSP PI data			
3				
4	Person	E-mail Address	MSP	MSP Start
5	Jane Doe	jane.do@gov.bc.ca	MSP	2007-06-15
6	Betty Boop	betty.boop@gov.bc.ca	MSP	2012-02-13
7	Clark Kent	clark.kent@gov.bc.ca	MSP	2007-06-15
8	Lois Lane	lois.lane@gov.bc.ca	MSP	2007-10-09
9	Rhett Butler	rhett.butler@gov.bc.ca	MSP	2013-07-16
10	Scarlette O'hara	scarlette.ohara@gov.bc.ca	MSP	2007-10-09
11	James T Kirk	james.t.kirk@gov.bc.ca	MSP	2008-12-19
12	Al Capone	al.capone@gov.bc.ca	MSP	2011-11-17
13	Ellitot Ness	elliott.ness@gov.bc.ca	MSP	2007-10-09

	A	B	C	D	E	F
1	Person	Email Address	Person_1	Container	Default	Active
2	AIJUN YANG	Aijun.Yang@gov.bc.ca	AIJUN YANG			
3	AIJUN YANG	Aijun.Yang@gov.bc.ca	AIJUN YANG			
4	ALICE XU	Alice.Xu@gov.bc.ca	ALICE XU			
5	ALICE XU	Alice.Xu@gov.bc.ca	ALICE XU			
6	ALICE XU	Alice.Xu@gov.bc.ca	ALICE XU			
7	ALLAN ROBERTSON	allan.robertson@gov.bc.ca	ALLAN ROBERTSON			
8	ALLAN ROBERTSON	allan.robertson@gov.bc.ca	ALLAN ROBERTSON			
9	ALLAN ROBERTSON	allan.robertson@gov.bc.ca	ALLAN ROBERTSON			
10	ALLAN ROBERTSON	allan.robertson@gov.bc.ca	ALLAN ROBERTSON			
11	ANATOLI SKRIPNITCHENKO	Anatoli.Skripnitchenko@gov.bc.ca	ANATOLI SKRIPNITCHENKO			
12	ANATOLI SKRIPNITCHENKO	Anatoli.Skripnitchenko@gov.bc.ca	ANATOLI SKRIPNITCHENKO			
13	ANATOLI SKRIPNITCHENKO	Anatoli.Skripnitchenko@gov.bc.ca	ANATOLI SKRIPNITCHENKO			
14	ANDREA GREGG	andrea.gregg@gov.bc.ca	ANDREA GREGG			
15	ANDREW SHAW	Andrew.Shaw@gov.bc.ca	ANDREW SHAW			
16	ANDREW SHAW	Andrew.Shaw@gov.bc.ca	ANDREW SHAW			
17	ANDREW SHAW	Andrew.Shaw@gov.bc.ca	ANDREW SHAW			
18	APRIL FELKER	april.felker@gov.bc.ca	APRIL FELKER			
19	BART JEDYNAK	Bart.Jedynak@gov.bc.ca	BART JEDYNAK			
20	BART JEDYNAK	Bart.Jedynak@gov.bc.ca	BART JEDYNAK			
21	BEVERLY WAN	beverly.wan@gov.bc.ca	BEVERLY WAN			
22	BEVERLY WAN	beverly.wan@gov.bc.ca	BEVERLY WAN			
23	BEVERLY WAN	beverly.wan@gov.bc.ca	BEVERLY WAN			
24	BRAD CORNER	bradley.corner@gov.bc.ca	BRAD CORNER			
25	BRENNA KELLN	Brenna.Kelln@gov.bc.ca	BRENNA KELLN			
26	BRENNA KELLN	Brenna.Kelln@gov.bc.ca	BRENNA KELLN			
27	CABIO TSE	Cabio.Tse@gov.bc.ca	CABIO TSE			
28	CABIO TSE	Cabio.Tse@gov.bc.ca	CABIO TSE			
29	CABIO TSE	Cabio.Tse@gov.bc.ca	CABIO TSE			
30	CARLOS CARAVEO	Carlos.Caraveo@gov.bc.ca	CARLOS CARAVEO			
31	CARLOS CARAVEO	Carlos.Caraveo@gov.bc.ca	CARLOS CARAVEO			
32	CAROL RITTER	carol.ritter@gov.bc.ca	CAROL RITTER			

s. 15

	G	H	I	J
1	Role	Default_1	Active_1	OID/LDAP dn
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				s. 15
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				

	A	B	C	D	E	F
1	Person	Email Address	Person_1	Container	Default	Active
33	CAROLYN RUDDEN	Carolyn.Rudden@gov.bc.ca	CAROLYN RUDDEN			
34	CHAD KAILA	Chad.Kaila@gov.bc.ca	CHAD KAILA			
35	CHRISTINE VOGGENREITER	christine.voggenreiter@gov.bc.ca	CHRISTINE VOGGENREITER			
36	CHRISTINE VOGGENREITER	christine.voggenreiter@gov.bc.ca	CHRISTINE VOGGENREITER			
37	CHRISTINE VOGGENREITER	christine.voggenreiter@gov.bc.ca	CHRISTINE VOGGENREITER			
38	CHRISTINE VOGGENREITER	christine.voggenreiter@gov.bc.ca	CHRISTINE VOGGENREITER			
39	CHRISTINE VOGGENREITER	christine.voggenreiter@gov.bc.ca	CHRISTINE VOGGENREITER			
40	CLNT BLUE MATRIX	Martha.Burd@gov.bc.ca	CLNT BLUE MATRIX			
41	CLNT BLUE MATRIX	Martha.Burd@gov.bc.ca	CLNT BLUE MATRIX			
42	CLNT BLUE MATRIX	Martha.Burd@gov.bc.ca	CLNT BLUE MATRIX			
43	DALE STARR	Dale.Starr@gov.bc.ca	DALE STARR			
44	DALE STARR	Dale.Starr@gov.bc.ca	DALE STARR			
45	DARCY DRAGSETH	Darcy.Dragseth@gov.bc.ca	DARCY DRAGSETH			
46	DAVE GARTON	dave.garton@gov.bc.ca	DAVE GARTON			
47	DAVID MAH	david.mah@gov.bc.ca	DAVID MAH			
48	DAVID MAH	david.mah@gov.bc.ca	DAVID MAH			
49	DAVID MAH	david.mah@gov.bc.ca	DAVID MAH			
50	DON RINTOUL	Don.Rintoul@gov.bc.ca	DON RINTOUL			
51	DON RINTOUL	Don.Rintoul@gov.bc.ca	DON RINTOUL			
52	EDWARD CHANG	Edward.Chang@gov.bc.ca	EDWARD CHANG			
53	EDWARD CHANG	Edward.Chang@gov.bc.ca	EDWARD CHANG			
54	EDWARD CHANG	Edward.Chang@gov.bc.ca	EDWARD CHANG			
55	ELAINE WOODWARD	elaine.woodward@gov.bc.ca	ELAINE WOODWARD			
56	ELLEN DRAGUSHAN	Ellen.Dragushan@gov.bc.ca	ELLEN DRAGUSHAN			
57	ERIC LARSON	Eric.Larson@gov.bc.ca	ERIC LARSON			
58	ERIC LARSON	Eric.Larson@gov.bc.ca	ERIC LARSON			
59	ERIC LARSON	Eric.Larson@gov.bc.ca	ERIC LARSON			
60	EVA JORDAN	eva.jordan@maximusbc.ca	EVA JORDAN			
61	EXTAPP MHR		EXTAPP MHR			
62	FANNY WONG	fanny.wong@gov.bc.ca	FANNY WONG			
63	FANNY WONG	fanny.wong@gov.bc.ca	FANNY WONG			
64	FANNY WONG	fanny.wong@gov.bc.ca	FANNY WONG			

s. 15

	G	H	I	J
1	Role	Default_1	Active_1	OID/LDAP dn
33				
34				
35				
36				
37				
38				
39				
40				
41				
42				
43				
44				
45				
46				
47				
48				
49				
50				
51				
52				
53				
54				
55				
56				
57				
58				
59				
60				
61				
62				
63				
64				

s. 15

	A	B	C	D	E	F
1	Person	Email Address	Person_1	Container	Default	Active
65	GARY KO	Gary.Ko@gov.bc.ca	GARY KO	s. 15		
66	GARY KO	Gary.Ko@gov.bc.ca	GARY KO			
67	GAY CORBETT	Gay.Corbett@gov.bc.ca	GAY CORBETT			
68	GAYLE WILSON	gayle.wilson@gov.bc.ca	GAYLE WILSON			
69	GORD STODOLA	Gordon.Stodola@gov.bc.ca	GORD STODOLA			
70	GORD STODOLA	Gordon.Stodola@gov.bc.ca	GORD STODOLA			
71	GORD STODOLA	Gordon.Stodola@gov.bc.ca	GORD STODOLA			
72	GORD STODOLA	Gordon.Stodola@gov.bc.ca	GORD STODOLA			
73	GORD STODOLA	Gordon.Stodola@gov.bc.ca	GORD STODOLA			
74	GORDON HANAKA	Gordon.Hanaka@gov.bc.ca	GORDON HANAKA			
75	GRACE LIN	Grace.Lin@gov.bc.ca	GRACE LIN			
76	GREG ABBOTT	Greg.Abbott@gov.bc.ca	GREG ABBOTT			
77	GREG ABBOTT	Greg.Abbott@gov.bc.ca	GREG ABBOTT			
78	GREG ABBOTT	Greg.Abbott@gov.bc.ca	GREG ABBOTT			
79	GUIXIANG ZHANG	guixiang.zhang@gov.bc.ca	GUIXIANG ZHANG			
80	GUIXIANG ZHANG	guixiang.zhang@gov.bc.ca	GUIXIANG ZHANG			
81	GUIXIANG ZHANG	guixiang.zhang@gov.bc.ca	GUIXIANG ZHANG			
82	HEATHER JENNINGS	Heather.Jennings@gov.bc.ca	HEATHER JENNINGS			
83	HEATHER JENNINGS	Heather.Jennings@gov.bc.ca	HEATHER JENNINGS			
84	HENRY TRAN	Henry.Tran@gov.bc.ca	HENRY TRAN			
85	HENRY TRAN	Henry.Tran@gov.bc.ca	HENRY TRAN			
86	HENRY TRAN	Henry.Tran@gov.bc.ca	HENRY TRAN			
87	JASON PLATT	Jason.Platt@gov.bc.ca	JASON PLATT			
88	JEMAL MOHAMED	Jemal.Mohamed@gov.bc.ca	JEMAL MOHAMED			
89	JEMAL MOHAMED	Jemal.Mohamed@gov.bc.ca	JEMAL MOHAMED			
90	JEMAL MOHAMED	Jemal.Mohamed@gov.bc.ca	JEMAL MOHAMED			
91	JEMAL MOHAMED	Jemal.Mohamed@gov.bc.ca	JEMAL MOHAMED			
92	JILDIZ SHABDANALIEVA	Jildiz.Shabdanalieva@gov.bc.ca	JILDIZ SHABDANALIEVA			
93	JILDIZ SHABDANALIEVA	Jildiz.Shabdanalieva@gov.bc.ca	JILDIZ SHABDANALIEVA			
94	JILDIZ SHABDANALIEVA	Jildiz.Shabdanalieva@gov.bc.ca	JILDIZ SHABDANALIEVA			
95	JIM YU	jim.yu@gov.bc.ca	JIM YU			
96	JIM YU	jim.yu@gov.bc.ca	JIM YU			

	G	H	I	J
1	Role	Default_1	Active_1	OID/LDAP dn
65				
66				
67				
68				
69				
70				
71				
72				
73				
74				
75				
76				
77				
78				
79				
80				
81				
82				
83				
84				
85				
86				
87				
88				
89				
90				
91				
92				
93				
94				
95				
96				

s. 15

	A	B	C	D	E	F
1	Person	Email Address	Person_1	Container	Default	Active
97	JIM YU	jim.yu@gov.bc.ca	JIM YU			
98	JINHWA OH	Jinhwa.Oh@gov.bc.ca	JINHWA OH			
99	JINHWA OH	Jinhwa.Oh@gov.bc.ca	JINHWA OH			
100	JOEL CHOY	Joel.Choi@gov.bc.ca	JOEL CHOY			
101	JOEL CHOY	Joel.Choi@gov.bc.ca	JOEL CHOY			
102	KENT MAYNARD	kent.Maynard@gov.bc.ca	KENT MAYNARD			
103	KENT MAYNARD	kent.Maynard@gov.bc.ca	KENT MAYNARD			
104	KENT MAYNARD	kent.Maynard@gov.bc.ca	KENT MAYNARD			
105	LAURIE CARDIFF	Laurie.Cardiff@gov.bc.ca	LAURIE CARDIFF			
106	LEE URQUHART	lee.urquhart@hibc.gov.bc.ca	LEE URQUHART			
107	LINDA STOREY	Linda.Storey@gov.bc.ca	LINDA STOREY			
108	LIPING ZHANG	Liping.Zhang@gov.bc.ca	LIPING ZHANG			
109	LIPING ZHANG	Liping.Zhang@gov.bc.ca	LIPING ZHANG			
110	LIPING ZHANG	Liping.Zhang@gov.bc.ca	LIPING ZHANG			
111	LISA PALFREY	lisa.palfrey@gov.bc.ca	LISA PALFREY			
112	LORINDA ATKINSON	Lorinda.Atkinson@gov.bc.ca	LORINDA ATKINSON			
113	LORINDA ATKINSON	Lorinda.Atkinson@gov.bc.ca	LORINDA ATKINSON		s. 15	
114	LORINDA ATKINSON	Lorinda.Atkinson@gov.bc.ca	LORINDA ATKINSON			
115	MAHINDER TAKHAR	Mahinder.Takhar@gov.bc.ca	MAHINDER TAKHAR			
116	MAHINDER TAKHAR	Mahinder.Takhar@gov.bc.ca	MAHINDER TAKHAR			
117	MARIA MIDDLEMISS	Maria.Middlemiss@gov.bc.ca	MARIA MIDDLEMISS			
118	MARILYN MARR	Marilyn.Marr@gov.bc.ca	MARILYN MARR			
119	MARJ HALLIHAN	Marjorie.Hallihan@gov.bc.ca	MARJ HALLIHAN			
120	MELISSA YAU	melissa.yau@gov.bc.ca	MELISSA YAU			
121	MENGHONG GAO	MengHong.Gao@gov.bc.ca	MENGHONG GAO			
122	MENGHONG GAO	MengHong.Gao@gov.bc.ca	MENGHONG GAO			
123	MICHAEL CHANG	Michael.Chang@gov.bc.ca	MICHAEL CHANG			
124	MICHAEL CHANG	Michael.Chang@gov.bc.ca	MICHAEL CHANG			
125	MICHAEL CHANG	Michael.Chang@gov.bc.ca	MICHAEL CHANG			
126	MICHAEL CHANG	Michael.Chang@gov.bc.ca	MICHAEL CHANG			
127	MICHELLE TSANG	Michelle.Tsang@gov.bc.ca	MICHELLE TSANG			
128	MICHELLE TSANG	Michelle.Tsang@gov.bc.ca	MICHELLE TSANG			

	G	H	I	J
1	Role	Default_1	Active_1	OID/LDAP dn
97				
98				
99				
100				
101				
102				
103				
104				
105				
106				
107				
108				
109				
110				
111				
112				
113				
114				
115				
116				
117				
118				
119				
120				
121				
122				
123				
124				
125				
126				
127				
128				

s. 15

	A	B	C	D	E	F
1	Person	Email Address	Person_1	Container	Default	Active
129	MIKE ATKINSON	mike.atkinson@gov.bc.ca	MIKE ATKINSON	s. 15		
130	MIKE ATKINSON	mike.atkinson@gov.bc.ca	MIKE ATKINSON			
131	MIKE ATKINSON	mike.atkinson@gov.bc.ca	MIKE ATKINSON			
132	MIKE ATKINSON	mike.atkinson@gov.bc.ca	MIKE ATKINSON			
133	MIKE ATKINSON	mike.atkinson@gov.bc.ca	MIKE ATKINSON			
134	MIKE ATKINSON	mike.atkinson@gov.bc.ca	MIKE ATKINSON			
135	MING GUO	Ming.Guo@gov.bc.ca	MING GUO			
136	MINOO BABRITERANI	minoo.babriterani@gov.bc.ca	MINOO BABRITERANI			
137	MONICA MCMILLAN	Monica.McMillan@gov.bc.ca	MONICA MCMILLAN			
138	MUHAMMAD ANWER	Muhammad.Anwer@gov.bc.ca	MUHAMMAD ANWER			
139	MUHAMMAD ANWER	Muhammad.Anwer@gov.bc.ca	MUHAMMAD ANWER			
140	NATALIA BARJASIC	Natalia.barjasic@gov.bc.ca	NATALIA BARJASIC			
141	NICK BYSTEDT	Nick.Bystedt@gov.bc.ca	NICK BYSTEDT			
142	NICK BYSTEDT	Nick.Bystedt@gov.bc.ca	NICK BYSTEDT			
143	NICK BYSTEDT	Nick.Bystedt@gov.bc.ca	NICK BYSTEDT			
144	NICOLE GILES	nicole.giles@gov.bc.ca	NICOLE GILES			
145	NICOLE GILES	nicole.giles@gov.bc.ca	NICOLE GILES			
146	NORA HUBER	Nora.Huber@gov.bc.ca	NORA HUBER			
147	OLIVIA YOUNG	Olivia.Young@gov.bc.ca	OLIVIA YOUNG			
148	PATRICK DAY	Patrick.day@gov.bc.ca	PATRICK DAY			
149	PATRICK DAY	Patrick.day@gov.bc.ca	PATRICK DAY			
150	PATRICK DAY	Patrick.day@gov.bc.ca	PATRICK DAY			
151	PAUL BRUNCKHURST	Paul.Brunckhurst@gov.bc.ca	PAUL BRUNCKHURST			
152	PAUL BRUNCKHURST	Paul.Brunckhurst@gov.bc.ca	PAUL BRUNCKHURST			
153	PAUL GILLAN	Paul.Gillan@gov.bc.ca	PAUL GILLAN			
154	PAUL LAM	Paul.Lam@gov.bc.ca	PAUL LAM			
155	PAUL LAM	Paul.Lam@gov.bc.ca	PAUL LAM			
156	PAUL LAM	Paul.Lam@gov.bc.ca	PAUL LAM			
157	PAUL YANG	Paul.Yang@gov.bc.ca	PAUL YANG			
158	PAUL YANG	Paul.Yang@gov.bc.ca	PAUL YANG			
159	PEIYU MEI	Peiyu.Mei@gov.bc.ca	PEIYU MEI			
160	QUINN SIRNA	Quinn.Sirna@gov.bc.ca	QUINN SIRNA			

	G	H	I	J
1	Role	Default_1	Active_1	OID/LDAP dn
129				
130				
131				
132				
133				
134				
135				
136				
137				
138				
139				
140				
141				
142				
143				
144				
145				
146				
147				
148				
149				
150				
151				
152				
153				
154				
155				
156				
157				
158				
159				
160				

s. 15

	A	B	C	D	E	F
1	Person	Email Address	Person_1	Container	Default	Active
161	QUINN SIRNA	Quinn.Sirna@gov.bc.ca	QUINN SIRNA			
162	RITA KING	Rita.King@gov.bc.ca	RITA KING			
163	ROB VON RUDLOFF	Robert.VonRudloff@gov.bc.ca	ROB VON RUDLOFF			
164	ROB VON RUDLOFF	Robert.VonRudloff@gov.bc.ca	ROB VON RUDLOFF			
165	ROB VON RUDLOFF	Robert.VonRudloff@gov.bc.ca	ROB VON RUDLOFF			
166	RON MERNER	Ron.Merner@gov.bc.ca	RON MERNER			
167	RUIXIA MU	Ruixia.Mu@gov.bc.ca	RUIXIA MU			
168	SANDRA FELTHAM	sandra.feltham@gov.bc.ca	SANDRA FELTHAM			
169	SHAUNA LAVOIE	Shauna.lavoie@gov.bc.ca	SHAUNA LAVOIE			
170	SHELLEY HSIEH	Shelley.Hsieh@gov.bc.ca	SHELLEY HSIEH			
171	STEVE RICKLEY	steve.rickley@gov.bc.ca	STEVE RICKLEY			
172	STEVE RICKLEY	steve.rickley@gov.bc.ca	STEVE RICKLEY			
173	STEVE RICKLEY	steve.rickley@gov.bc.ca	STEVE RICKLEY			
174	STEVE RICKLEY	steve.rickley@gov.bc.ca	STEVE RICKLEY			
175	SUSAN CHAYTOR	Susan.Chaytor@gov.bc.ca	SUSAN CHAYTOR			
176	SUSAN CHAYTOR	Susan.Chaytor@gov.bc.ca	SUSAN CHAYTOR			
177	THERESA EDISON	Theresa.Edison@gov.bc.ca	THERESA EDISON			
178	THERESA EDISON	Theresa.Edison@gov.bc.ca	THERESA EDISON			
179	TIM HISTER	tim.hister@gov.bc.ca	TIM HISTER			
180	TIM JEPP	Tim.Jepp@gov.bc.ca	TIM JEPP			
181	TIM JEPP	Tim.Jepp@gov.bc.ca	TIM JEPP			
182	TIM JEPP	Tim.Jepp@gov.bc.ca	TIM JEPP			
183	TIM JEPP	Tim.Jepp@gov.bc.ca	TIM JEPP			
184	TONY WANG	Tony.Wang@gov.bc.ca	TONY WANG			
185	TONY WANG	Tony.Wang@gov.bc.ca	TONY WANG			
186	TONY WANG	Tony.Wang@gov.bc.ca	TONY WANG			
187	TRACY CONNETT	Tracy.Connett@gov.bc.ca	TRACY CONNETT			
188	TREENA TOTH	Treena.Toth@gov.bc.ca	TREENA TOTH			
189	TYLER BLONDE	tyler.blonde@gov.bc.ca	TYLER BLONDE			
190	VERN MCINTOSH	Vern.McIntosh@gov.bc.ca	VERN MCINTOSH			
191	VIJAY VYAS	Vijay.Vyas@gov.bc.ca	VIJAY VYAS			
192	VIJAY VYAS	Vijay.Vyas@gov.bc.ca	VIJAY VYAS			

s. 15

	G	H	I	J
1	Role	Default_1	Active_1	OID/LDAP dn
161				
162				
163				
164				
165				
166				
167				
168				
169				
170				
171				
172				
173				
174				
175				
176				
177				
178				
179				
180				
181				
182				
183				
184				
185				
186				
187				
188				
189				
190				
191				
192				

s. 15

	A	B	C	D	E	F
1	Person	Email Address	Person_1	Container	Default	Active
193	VIJAY VYAS	Vijay.Vyas@gov.bc.ca	VIJAY VYAS			
194	XIAOYUN SUN	Xiaoyun.Sun@gov.bc.ca	XIAOYUN SUN			
195	YONGCAI LIU	Yongcai.Liu@gov.bc.ca	YONGCAI LIU			
196	YONGCAI LIU	Yongcai.Liu@gov.bc.ca	YONGCAI LIU		s. 15	
197	YONGCAI LIU	Yongcai.Liu@gov.bc.ca	YONGCAI LIU			
198	ZHIYING SONG	zhiying.song@gov.bc.ca	ZHIYING SONG			
199	ZHIYING SONG	zhiying.song@gov.bc.ca	ZHIYING SONG			

	G	H	I	J
1	Role	Default_1	Active_1	OID/LDAP dn
193				
194				
195				
196				s. 15
197				
198				
199				

HSIMT

Ministry of Health

Title: Data Access managed outside of the Health Sector Information Management and Technology (HSIMT) Division

Approved by: Chief Data Steward

Policy source: Manager, Health Data Access Services

Effective: Next Date Review:

Policy Statement:

Owners or managers of data sets not managed by HSMIT must comply with Office of the Chief Information Officer (OCIO) guidelines and Ministry policy regarding access management of data sets.

In order for the ministry to ensure that access to its data sets continue to meet best practice standards the respective program Director will be the data access approver.

Access to data is tied to the position, not to the individual. The Director is responsible for approving an individual's initial access, based upon either the position occupied, or for a particular time limited project requirement.

The Director is responsible for locking access when an individual with access goes on leave of any kind, such as a Temporary Assignment, Educational Leave, STIIP, LTD or other leave longer than two weeks. This access can be unlocked when that the individual returns to the same position and job duties they left.

The Director is responsible for terminating access when an individual leaves a position (e.g. takes a position outside of the office, retires, is dismissed, etc), or the nature of the position changes such that access is no longer required to perform the new job duties, or when the particular time limited project is completed.

Access must be locked or removed within 5 business days of the individuals change in status.

Good access management requires that the following access information be captured:

- Name of individual access being granted to, date of access, name of data set, date access locked, date access terminated, who approved the access, level of access if this exists, etc.
- This information needs to be kept in accordance with corporate records management policy so that it is accessible for audit purposes.

Scope:

Only Director level staff and above can authorize data access requests for applicants within their work unit.

Guidelines:

The right to have access to data is linked to the job functions inherent in the position (i.e. the access to the specific data is required by that position in order to perform the job functions, or for a specific, time-limited project).

Industry best practices for access to data that are personally identifiable (PI) or sensitive rest on the principles of 'least privilege' and 'need to know'. In simple terms, the intention is to enable the provision of the right data, to the right person, at the right time.

Reference: (optional)

OCIO Information Security Policy, Chapter 7 Data Access

<http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf>

HSIMT

Ministry of Health

Title: Role of Divisional Data Officer outside of Health Sector and Information Management Technology (HSIMT) Division

Approved by: Chief Data Steward

Policy source: Manager, Health Data Access Services

Effective: Next Date Review:

Policy Statement:

Divisional Data Officers (DDOs) represent each Division's interests in relation to data management and governance and serve as the accountable party for ensuring that data governance requirements, including principles, policies and standards, are operationalized within their division.

Data Officers are responsible for controlling access to their program area data.

Granting access to specific data are based upon the requirements of an ongoing job function, or for the duration of a specific time-limited project.

Good access management requires that the following access information be captured:

- Name of individual access being granted to, date of access, name of data set, date access locked, date access terminated, who approved the access, level of access if this exists, etc.
- This information needs to be kept in accordance with corporate records management policy so that it is accessible for audit purposes.

Data Officers are also responsible for ensuring an access review occurs whenever there is a significant re-organization within the division. Access reviews should occur at least annually even if there has been no divisional re-organization.

Scope:

Each division has a designated Divisional Data Officer, appointed by the respective senior representative of the division (ADM)

Background:

The Office of the Information and Privacy Commissioner requires the ministry to have written policy concerning data access.

Guidelines:

Best practices for access to data that are personally identifiable or sensitive rests on the principles of “least privilege” and “need to know”. In simple terms, the intention is to enable the provision of the right data, to the right person, at the right time.

Reference:

OCIO Information Security Policy, Chapter 7 Data Access

<http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf>

Ministry of Health**IM/IT POLICY MANUAL**

Title: Data Access Policy
Effective: XXXX

Policy

This policy provides a framework for consistent management of access to data under the control of the Ministry of Health (the "Ministry").

Access to Ministry data must be consistent with the provisions of the *Freedom of Information and Protection of Privacy Act* (FIPPA), the *Document Disposal Act*, other relevant legislation, and other government policies such as the *Core Policy and Procedures Manual*.

Confidentiality and privacy

Access to data by Ministry employees must be for the least amount of data necessary on a need-to-know basis. Employees are not entitled to access merely because of status, rank or office.

Authority to grant access – Internal to Ministry

The Chief Data Steward (CDS) or delegate will approve data use and disclosure to Ministry employees requesting access. Appropriate records must document all requests and approvals.

Dispute regarding access by employees may be referred to the CDS.

Authority to grant access – External to Ministry

The CDS will approve data disclosure to external clients requesting access. Appropriate records must document all requests and approvals. The CDS will keep and record copies of data access agreements.

Notwithstanding the above, the Director of Vital Statistics will approve access to vital statistics data as authorized and required in the *Vital Statistics Act* and regulations.

Data integrity

All data access approvals must incorporate reasonable security arrangements to ensure that the authority to use, disclose, change or delete Ministry data is restricted to authorized individuals.

Audit trails and compliance monitoring

When appropriate to the value and sensitivity of the information, an audit trail of data access, including modifications or deletions to Ministry data, will be required. The audit trail will identify: who accessed the data, what data was accessed, when the data was accessed.

The Ministry has the right to perform unannounced audits and inspections to confirm compliance with terms and conditions of data access agreements.

Shared control of data

Where the Ministry and one or more other person or corporate body have the ability to update/amend data, one party will assume and document the primary responsibilities for control including data access, use, disclosure, security, modification, retention, and disposition.

Contractors

Contractors to the Ministry (including all employees and subcontractors of the contractor) must be bound by confidentiality undertakings to ensure the confidentiality of Ministry data and the privacy of individuals.

Fees

Ministry of Health

IM/IT POLICY MANUAL

Where consistent with legislation and policy, the Ministry may charge a fee for data access.

Agreements

Except as specified in the following matrix, all access to Ministry data must be authorized an agreement.

Insofar as is practical, the Ministry will have a single, standardized agreement with each person or corporate body. A single agreement may authorize access to data from several Ministry program areas. Agreements may be amended from time to time and may include schedules dealing with access to specific data or the use of specific systems.

In some cases, a Privacy Impact Assessment (PIA) may be required, please contact the provincial Chief Information Officer (CIO) staff or website for further information.

The type of data user, the category of data, and the purpose for accessing the data determine whether an agreement is required:

Type of data users / Client	Agreement Required (Y/N)
Individuals requesting their own personal information	No agreement required Use CIO FOI guidelines
Any person or corporate body requesting access to routinely releasable non sensitive information: documents, files or records series containing only information that would be released to any member of the public	No agreement required Use CIO guidelines
Ministry employees: Internal use	No agreement required Grant access to the operational data or to a copy, as appropriate to the operational needs, employee's job function and need-to-know. Notes: The confidentiality of this type of access is covered by an employee's Oath of Office.
Health Authorities and their agencies	Yes, agreement required Exception: Where express legislative authority exists, agreement may not be required.
Public Bodies (i.e. other ministries)	Yes, agreement required. Exception: Where express legislative authority exists, agreement may not be required.
Federal Partners (i.e. Health Canada)	Yes, agreement required. Exception: Where express legislative authority exists, agreement may not be required.
Private and/or non-profit bodies	Yes, agreement required Exception: Where express legislative authority exists, agreement may not be required.

Background

This policy applies to all data under the custody and control of the Ministry.

Ministry of Health**IM/IT POLICY MANUAL**

This policy recognizes legislated responsibilities and authorities for the management of vital statistics data that are defined in the *Vital Statistics Act*.

ROLES AND RESPONSIBILITIES**Chief Data Steward**

- Ensure that this policy is implemented within their area of responsibility.
- Approve agreements on behalf of the Ministry. This authority may be delegated for data access for classes of users, such as health authorities.
- Develop and maintain Ministry policies, standards, guidelines and procedures regarding information management, including data access.
- Undertake ongoing compliance monitoring and reporting on implementation of this policy.
- Undertake periodic reviews of access authorizations for the purpose of terminating expired or inappropriate access authorizations
- Maintain a registry of ministry agreements.

Director of Vital Statistics

Approve access to vital statistics data as authorized and required in the *Vital Statistics Act* and regulations.

Glossary of Terms

- **Access (to data):** means the authority and the ability to apprehend or collect data, electronically or otherwise.
- **Chief Data Steward:** means the official responsible for managing Ministry data, whose responsibilities include managing data creation or acquisition, completeness, currency, integrity, storage, protection and disposition, as well as access to data.
- **Control (of data):** means the power or authority to manage, restrict, regulate or administer the creation, acquisition, use or disclosure of data. Indicators of control of data include responsibility for creation, acquisition, management, retention and disposition, or access to data.
- **Data:** means a recorded representation of a fact, regardless of the medium in which it is recorded.
- **Data Access Agreement:** means an agreement that authorizes access to Ministry data by people or corporate bodies external to the Ministry and which is used to manage that data access.
- **Data Integrity:** means the preservation of content throughout collection, storage, use, transfer, disclosure, and retrieval so that there is confidence that data has not been tampered with or modified except as authorized.
- **Disclosure:** means data that is released from the Ministry so that it can be used by the signatories according to the DAA authorizing the release.
- **Employee:** means employee or contractor of the Ministry.
- **External to Ministry:** Means persons or corporate bodies who are not employees or contractors of the Ministry.
- **Information:** means the meaning of interpreted data. Data becomes information when it is perceived in context and conveys meaning.
- **Ministry data:** means data controlled by the Ministry.
- **Need-to-know:** means the security principle that access to data is restricted to authorized individuals whose duties require such access.
- **Use:** means data used within the Ministry for internal operational purposes.

Below is a copy of the online Add Team Member Application form on the Population Data BC website. The online form can be found at http://www.popdata.bc.ca/forms/add_team_member

Addition of Team Member(s) Application Form

Please note: Once all approvals are in place, Principal Investigator/Applicant must meet the following requirements. Additional study team members will not be given data access until all requirements are met:

- 1 Updated ethics documents with new team members' names being listed
- 2 Signed Pledge of Confidentiality (if accessing data)
- 3 Successful completion of Privacy Training (if accessing data)

PROJECT INFORMATION

Project number: *

Project title: *

Principal Investigator/Applicant: *

ADDITIONAL STUDY TEAM MEMBERS Additional team member 1

Name: *

Position: *

Affiliation: *

Role (e.g. Co-investigator, Analyst): *

Need data access?: *

☐

Yes

☐

No

Additional team member 2

Name:

Position:

Affiliation:

Role (e.g. Co-investigator, Analyst:

Need data access?:

☐ Yes

☐ No

Additional team member 3

Name:

Position:

Affiliation:

Role (e.g. Co-investigator, Analyst:

Need data access?:

☐ Yes

☐ No

Additional team member 4

Name:

Position:

Affiliation:

Role (e.g. Co-investigator, Analyst:

Need data access?:

☐ Yes

☐ No

Data Access Request (DAR) manual

Last revised: November 2012

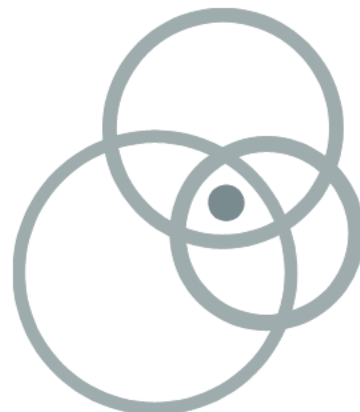


TABLE OF CONTENTS

PLANNING AND COMPLETING A DATA ACCESS REQUEST.....	3
SECTION I: APPLICATION DETAILS	5
SECTION II: APPLICATION SUBMISSION PROCESS	5
SECTION III: FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (FIPPA)	6
SECTION IV: PREVIOUSLY APPROVED DATA REQUESTS RELEVANT TO THE APPLICATION	6
SECTION V: REQUEST TO CONTACT	7
SECTION VI: REQUIRED DOCUMENTATION CHECKLIST	7
SECTION VII: APPLICANT AND RESEARCH TEAM INFORMATION.....	8
SECTION VIII: FUNDING, AFFILIATIONS, AND REVIEWS	10
SECTION IX: RESEARCH PROJECT DESCRIPTION	11
SECTION X: DEFINING YOUR STUDY POPULATION	13
SECTION XI: DATABASES USED FOR EXTRACT	14
SECTION XII: DATA LINKAGE BETWEEN POPULATION DATA BC AND EXTERNAL DATA.....	16
SECTION XIII: DATA SECURITY AND ACCESS.....	18
SECTION XIV: SIGNATURE AND DECLARATION	19
IN CLOSING	20

The Data Access Request application form (DAR) has been developed and approved by Population Data BC (PopData) and its Data Steward partners. It is intended to be used to request data administered by PopData as well as for data requests that involve linkage to external data. The DAR form is meant to stand alone. It should contain all the information required to support an application and should contain a complete description of the project.

All requests for data are adjudicated by Data Stewards who, in turn, are bound by BC's *Freedom of Information and Protection of Privacy Act* (FIPPA) and other relevant laws and regulations of the Province, and ethical guidelines. PopData works on behalf of Data Stewards and Applicants to help with the process, but has no role in the actual adjudication of requests.

Access to data through PopData is governed by the Research Data Access Framework (RDAF) which outlines the principles and the responsibilities involved in the data access request process. Applicants are encouraged to familiarize themselves with the RDAF before submitting applications for data. Visit: www.popdata.bc.ca/dataaccess/rdaf for more information on the RDAF.

PLANNING AND COMPLETING A DATA ACCESS REQUEST

Why is a DAR form needed?

Data Stewards require specific information about your project in order to adjudicate on it. PopData staff will also need specific information in order to prepare data, once a DAR is approved. The DAR is designed to collect and present this information in the most efficient manner possible for adjudication.

A summary of the DAR process

The data access request process is dependent on, but separate from, funding and ethics. Applicants will need to have funding in place and an approved ethics certificate. Data access approval is not automatic and must be taken as seriously as an application for funding or ethical review. Completing a DAR takes time, planning, and attention to detail, as they are reviewed thoroughly.

The application process requires that the Applicant:

- Become familiar with all material outlining access requirements, data holdings, study population definitions, and privacy considerations, as presented on the PopData website.
- Ensure that the ethics and peer review requirements of the Data Steward(s) have been met.
- Ensure that the appropriate application, approvals and Research Agreements are sought, (including linkage requirements) if external data is to be used.
- Submit a completed DAR to PopData, including **ALL** required attachments.
- Work with PopData to complete the Study Population description and discuss linkages.

Please visit PopData's website FAQ sections for more information. Questions about the application process, or any part of the application, are to be directed to the staff in PopData's Researcher Liaison Unit (RLU) at: rlu@popdata.bc.ca.

Once the DAR form has been reviewed and all necessary approvals are in place, a Research Agreement must be signed by the Applicant and Principal Investigator (PI) (if different from the Applicant) as well as the applicable Data Steward(s). This is a legal agreement between the public bodies that the Data Steward(s) represent and the Applicant and/or PI. The DAR form will become an appendix to the Research Agreement.

How to complete the form

The DAR form has been setup as a PDF 'form-fill' application with the document text being protected from inadvertent changes. Checkboxes may be checked by clicking with a mouse or using the space bar.

SECTION I: APPLICATION DETAILS

The Applicant and Principal Investigator

Additional information on the Applicant and PI is located in SECTION VII: APPLICANT AND RESEARCH TEAM INFORMATION.

Project Title

Additional information on the Project Title is located in SECTION IX: RESEARCH PROJECT DESCRIPTION.

Student requests

There are two types of student data access requests.

- 1. A request to access existing Applicant data for the purpose of completing a thesis or dissertation**

Student's requesting access to existing project data must state the project number here. This type of request does not require that the student complete the entire DAR form; there will be no new data extracted as students will be granted access to an existing Research Extract. Please refer to the Student DAR Manual located on our website.

- 2. A stand-alone student request**

For stand-alone student requests, the student is required to complete the entire DAR form and fulfil all the requirements of the application form. In this scenario the student will be provided with their own Research Extract. No other parties are permitted to use the Research Extract under a student application for their own means or research materials. That is, use of student data for any other purpose than in support of the student's thesis/dissertation/project is prohibited.

For all student requests it is expected that the project (or student portion of the project) be closed upon completion of the thesis or dissertation.

SECTION II: APPLICATION SUBMISSION PROCESS

Applicant should read, and be familiar with, the application submission process and materials available on the PopData website at: www.popdata.bc.ca.

It is extremely important that Applicants ensure consistency on **ALL** project documentation and attachments. Applications with inconsistencies in project title, research team, research objectives, study population description, data linkages, dates and date ranges will be returned by the RLU. Applications with inconsistencies will not be submitted to the relevant Data Steward(s) until efforts by the Applicant have been made to ensure that the DAR and ethics application, for example, are consistent.

Inconsistencies are a major source of delay and frustration for the research team as well as the RLU. Please ensure that the same time and effort is spent to complete the DAR package as would be put towards a funding or ethical review application.

SECTION III: FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (FIPPA)

PopData would like to publish information about approved research projects whose data PopData administers, including on the PopData website. The purpose of this documentation (such as Applicant's name, project title and summary) is to provide information to the public and prospective Applicants about the types of research projects PopData facilitates. Please indicate on the form consent for use of none, all, or part of the described personal information collected on the application.

Please note that the consent to publish project information is voluntary and may be withdrawn at any time, for any reason, by contacting PopData.

SECTION IV: PREVIOUSLY APPROVED DATA REQUESTS RELEVANT TO THE APPLICATION

If the current request is related to a previously approved data release or data access request from PharmaNet or the Ministry of Health (including holdings at PopData) please indicate it in this section.

Please note either the PharmaNet (Data Stewardship Committee (DSC)) project number(s) or the Ministry of Health DAR project number in the space provided.

Please explain the relationship to the previously approved study. For example, if this is a student request to access existing applicant data please describe this relationship.

Example Relationship 1: I am a graduate student applying to use the MSP and WorkSafeBC data provided in the Research Extract for the approved project 00-000 Smith in order to fulfil the dissertation portion of my PHD studies. I will be analyzing these data to answer the following approved research question <<state approved research question here>>.

Example Relationship 2: I have applied previously to the Data Stewardship Committee (DSC) for PharmaNet data. My approved project number is 1900-00. I am now applying to the Ministry of Health for permission to link MSP and DAD (Hospital Separations) data to my existing approved PharmaNet data.

SECTION V: REQUEST TO CONTACT

All requests to use data for the purposes of contacting individuals to request their participation in health research must be reviewed and approved by the BC Information and Privacy Commissioner through the Data Stewardship Committee.

Please indicate in this section if the Applicant will be making a request to contact individuals included in the study for any reason. If so, please refer to the Request to Contact Potential Study Participants form which will soon be available on the PopData website.

SECTION VI: REQUIRED DOCUMENTATION CHECKLIST

This section has two purposes:

1. To assist Population Data BC and the Data Steward(s) in assessing the content and completion of the DAR package.
2. To assist the Applicant in organizing and compiling the necessary components of the application.

For convenience, each item on the checklist links to the section of the DAR from which it originates.

If the Applicant requires assistance or clarification regarding this checklist or completeness of the DAR, questions should be forwarded to the RLU.

Please ensure that each piece of documentation is consistent with the DAR form. If this is not possible, an explanation must be provided. Please check to ensure that consistent project title, research team, research objectives, study population description, data linkages, dates and date ranges are presented in each attachment.

Applications that are not complete will not be submitted to Data Stewards for review.

REQUIRED DOCUMENTATION

The attachments listed in this section are required for **ALL** projects.

IF NOT PEER REVIEWED

This section allows for submission of a letter from a supervisor (for student applications only) or a CV of the Applicant if no peer review has been performed.

ADDITIONAL DOCUMENTATION AS APPLICABLE

Items on this portion of the checklist can be filled in as applicable to the project.

For requests involving external data, special attention should be given to the required documentation. This documentation may include copies of other applications and Research Agreements for the external

data to which the Applicant wishes to link; and an approved copy of the informed consent letter that will be used for study recruitment.

Please ensure that all external data approvals clearly state the following, as applicable:

- Project title
- Applicant name and PI name if different from the Applicant
- Linkage (which databases will be linked for the project)
- Refer to the external list of variables
- Extract and/or cohort time period
- SRE storage approval
- Study population definition
- Approval of the linkage strategy

SECTION VII: APPLICANT AND RESEARCH TEAM INFORMATION

This section outlining the research team should match the approved Research Ethics Board (REB) application for the project exactly.

Applicant

The Applicant must be a person who is listed as the Principal Investigator or Co-Investigator in the REB approval (or official waiver process) from an accredited ethics review board, such as at a university or hospital. If the project is a thesis or dissertation, the Applicant must be the student.

The Applicant, as well as the PI (if different from the Applicant), is legally and ethically responsible for the data and the person with whom the Data Steward(s) will enter into a Research Agreement (RA). In the event of a breach, the Applicant will be held personally and professionally accountable to the Research Agreement (of which the DAR is an appendix).

The Applicant:

- Can only be a single individual. Although he/ she may be one of a number of Investigators on a grant/ethics application, one must be selected to be the Applicant.
- Can appoint another person to be the primary contact for the duration of the project.
- Is the person with whom Population Data BC will communicate during the application and approval process, unless otherwise delegated.

Principal Investigator

The Principal Investigator is an individual who either has a faculty appointment (Clinical Assistant Professor, Clinical Associate Professor, Clinical Professor, Assistant Professor, Associate Professor, Professor or BCCA Investigator) or is deemed a PI by an affiliated institution or by a Dean. This individual bears the overall responsibility for the conduct of the study, including the activities of the Co-

Investigators, who are assumed to be acting under the delegated authority of the PI, and is required to act within the requirements of the Tri-Council Policy Statement (TCPS).

The Principal Investigator must also be the Principal Investigator listed on ethics approval or waiver and in approvals for use of other data.

The PI, as well as the Applicant, is legally and ethically responsible for the data and the person with whom the Data Steward(s) will enter into a Research Agreement (RA). In the event of a breach, the PI will be held personally and professionally accountable to the Research Agreement (of which the DAR is an appendix).

Project Coordinator/Manager

A Project Coordinator/Manager may be appointed by the Applicant. This designate will be considered to be the primary contact person for the duration of the Agreement. The Project Coordinator will receive copies of all correspondence.

Co-Investigators

The name, position, and institutional affiliation of each Investigator on the research project must be provided. This is expected to mirror the Investigator list on the ethics certificate and the grant, if grant funding is in place.

Thesis/Dissertation Supervisor(s)

If data are to be used for a thesis or dissertation, the Applicant (the student) must provide the name, title, position, institution and contact information of their supervisor.

Persons who will have access to the data

Identify **ALL INDIVIDUALS** who will have access to the requested data at any time. Please include any of the Applicant, Principal Investigator, Project Coordinator/Manager, Co-Investigators and Thesis/Dissertation Supervisors on this list if they will be accessing the research extract. The name, position, institutional affiliation and email address of each is required.

In cases where access via the Secure Research Environment (SRE) is requested, this list will indicate only the individuals who will receive SecurIDs and be authorized to have access to the data.

Each person on this list will be required to a) sign a confidentiality pledge, and b) complete PopData's privacy training prior to release of data.

This list should be kept up to date with PopData. Adding or deleting individuals from this list is permitted and therefore both the RLU and Data Stewards must be kept informed about all changes in access. It may be necessary to amend the appropriate section of the ethics application to identify new individuals with data access.

SECTION VIII: FUNDING, AFFILIATIONS, AND REVIEWS

1. Who is funding your research project?

The Applicant must identify **ALL** funding, commissioning and contracting sources, including those requested but not yet confirmed. Please include the funder and the expiry date of funding.

If the project is funded by contract, Applicants must attach a copy of the contract, removing financial information.

Please be advised of the requirement that if an Applicant is funded by a for-profit organization, the industry sponsor must not influence analysis, or be given access to the data except in the final published results. Be aware of these rules if you negotiate a contract with an industry sponsor for a research project that requires access to data administered by PopData. Receiving funding that is considered a conflict of interest for the Data Providers involved in the request may mean result in the DAR being denied.

Non-student Applicants may not proceed with DAR applications before funding is secured. If grant funding is not yet secured, or in the case that grant funding is unsuccessful, Applicants are required to show proof of financial support, in order to proceed with the DAR process. Applicants must still show proof of peer review in order to satisfy DAR requirements.

If, at any time, before the research project is complete, the Applicant identifies a new patron or relationship with a funder, the Applicant must notify the RLU in writing.

All conflict of interests must be disclosed.

2. External peer review

Applicants must indicate the type of external peer review, and provide the necessary documents as indicated.

If a project has not been peer-reviewed, the Applicant must attach a complete CV to prove that the Applicant has the expertise to meet the objectives of the project.

3. Ethical review

Applicants must indicate the organization, certificate number and expiry date of the research project's ethical review by an REB, Institutional Review Board, or other institutional ethics review committee, and provide the necessary documents as indicated.

As stated on the DAR, only non-profit ethics review committees, such as those at universities, are acceptable. The Data Steward(s) reserve the right to decide the acceptability of ethics review committees. If the project has not been approved or submitted for review by an acceptable ethics review committee, the application will not be submitted to the Data Stewards.

Ethical reviews are updated periodically. It is the responsibility of the Applicant to ensure that any updates to ethical review are provided to PopData who will, in turn, share them with the Data Steward(s).

SECTION IX: RESEARCH PROJECT DESCRIPTION

Project title

The Applicant must indicate the complete title of the research project in the field provided. This should be the same title used on **ALL** other supporting documents attached to the DAR, for example, the ethics review or the funding application/peer review.

Title difference

If there is discrepancy amongst titles used on other supporting documents, the Applicant must state the reasons for this in the box provided.

Public interest value/public benefit of project

The Data Steward(s) readily support high-quality research on human health, well-being and the development of British Columbians and welcome research proposals aiming to inform policy-making that lead to healthier BC communities. As stipulated in FIPPA, the Data Steward(s) will assess projects with an eye for public interest value, and relevant legislation.

Small cell size

It is necessary to describe measures that will be taken to protect confidentiality (identification of an individual) during analysis and in any publication or distribution of results when dealing with small cell size. Please be sure to describe measures to be taken during analysis as well as in publication of results.

Examples of measures to be taken during analysis:

- Secure storage of the data on the SRE which involves controlled access for only individuals specified in the DAR.
- Privacy training is required for all team members accessing the data.
- Request for de-identified data, no identifiers will be retained for analysis.

Examples of measures to be taken during publication:

- Only aggregate results will be reported.
- Cell size of less than five individuals will not be reported.

Description of the project

The Applicant must provide a brief description of the project including its purpose and background. This should include an introduction to the project and a relationship to any other study program of research.

The Applicant must provide details of any relationship to other on-going studies. A general description of an area of investigation such as “to create a database on the health of health care workers” is not permissible.

Please note that FIPPA requires that Data Steward(s) approve access to data on a “need to know” basis for specific purposes only. As such, the research objective(s) will always be measured against the specific data requested.

Research objectives: research questions and hypotheses

Applicants must list **ALL** anticipated research objectives and questions, and should be as specific as possible. Consideration should be given to ‘preliminary’ research questions; re-workings of any hypotheses; and any theoretically ‘predictable’ outcomes of the analysis when designing the set of research questions.

The Data Steward(s) assess research questions in accordance with current provincial and national laws, regulations, and ethical standards. Research questions are reviewed for public interest value and compliance with legislation and policy, particularly the BC *Freedom of Information and Protection of Privacy Act* (FIPPA), and the Tri-Council Policy Statement for guidelines involving ethical research on humans.

Remember, upon approval and receipt of data, all analyses need to be restricted to those needed to answer these stipulated research questions. Any change in direction or scope of the question needs to be brought back for Data Steward review and approval, and may constitute a new project (requiring a new application and new data extract.)

Methodology

Applicants must summarize the study design and methodology including all statistical procedures within the analysis plan.

Please outline the techniques and the methodologies that will be employed and provide clear rationales for the appropriateness of the research design and methods.

Achieving research objectives

Under FIPPA section 35, the Data Steward(s) (and in turn Population Data BC) are permitted to release only those data that are necessary to achieve a specific research objective. It is the responsibility of the Applicant to draw this connection. Reviewers expect to see solid rationales outlining the relationship between the question(s) and the data requested. This section is expected to be fairly detailed in nature. It is necessary to identify each data file being requested, including external data files, and describe why each file is necessary to achieve the research objectives. It is recommended that this be filled out as one of the last sections, after the study population and checklists are complete.

SECTION X: DEFINING YOUR STUDY POPULATION

Each Applicant must collaborate with PopData on this section of the DAR before formal submission to the Data Steward(s). Applicants are advised that any changes to the study population post-approval will incur a fee in addition to any previous estimates or costs paid. Changes to the definition post-approval will also require a new Data Steward review.

To reiterate from the DAR, a study population is the group of subjects that a researcher wants to include in their analyses. The study population may include multiple cohorts as well as one or more comparison group(s).

In order to clarify on what is meant by ‘study population’, the table below provides a few examples of study populations, and how these relate to cohort(s), comparison group(s) and the data extract that might be requested for analyses.

Study population	Cohort	Comparison group(s)	Data extract
All women who gave birth in a BC hospital between 1993 and 2000, and their babies	Women who gave birth between 1993 and 2000 who are residents of Greater Vancouver	Women who gave birth between 1993 and 2000 who are residents of other parts of BC	All MSP Services, hospital separations and deaths data for mothers, from one year before to two years after birth. Births data for the babies, plus all MSP Services, hospital separations and deaths data for two years after birth.
All children for whom there are Early Development Instrument scores in 1999-2002 and 2007-2008	Kids with EDI scores above the median	Kids with EDI scores below the median	Foundation Skills Assessment scores, other education information, and hospitalizations for 1999 to 2008.
All individuals aged 65 and over who spent at least one night in a residential care facility between 1 April 1998 and 31 March 2008, plus a 10% random sample of other individuals aged 65 and over.	Individuals 65 and over who spent at least one night in a residential care facility between 1 April 1998 and 31 March 2008.	A 10% random sample of individuals who did not spend a night in a residential care facility but who were 65+ and resident in BC at some point between 1 April 1998 and 31 March 2008.	Home and Community Care, MSP Services, and Hospital Separations data for 1998/99 to 2007/08.

Although Applicants may have identified more than one cohort and/or comparison group in order to answer the research question, the data extract will contain the data covering the entire study population defined earlier. This will ensure that Applicants have all the data necessary to look at the cohort and comparison groups.

1. Who is creating the study population?

The cohort(s) or comparison group(s) for the study can be defined by data from PopData and/or by external data (from an external Data Provider or researcher-collected data). Please indicate the specifics of this in the checkboxes provided. This provides the Data Stewards with a quick context for their review of the study population section.

2. Text description

Applicants must define their study population in text and use as much detail as possible. These details should include any information to assist PopData in creating the study population. At this point, full descriptions of cohort(s) and comparison group(s) are helpful including inclusion and exclusion criteria.

3. Rationale for study population in relation to research objectives

A rationale or justification for the data requested must be provided. In this section, the focus is **ONLY** on the study population. In particular, justification of the breadth or specificity required to complete the research questions and objectives.

If requesting a population-based cohort, please provide a strong rationale as to why the research objectives cannot be met by sampling or by using a sub-set of the population.

SECTION XI: DATABASES USED FOR EXTRACT

Applicants must download and complete the appropriate data file checklist(s) and select the fields to be used for analysis.

Applicants need to request the data for their extract and not the data required to construct a study population when filling out the data file checklists.

The Data Steward(s) will assess each and every field to determine how each field pertains to the project objective. Justification for the fields should be provided by the Applicant in Section IX: Achieving Research Objectives of the DAR.

Applicants are encouraged to use all available resources, such as information provided on the PopData website, discussions with RLU staff, and consultations with other successful Applicants.

Neither the Data Steward(s) nor PopData will be held responsible for data selection oversights. The onus is on the Applicant to identify and investigate data holdings prior to submitting an application for data.

Applicants may request data to the end of the current year only (fiscal or calendar year).

1. Internal data request

Applicants are required to fill in the tables in the DAR form specifying with a check mark each data file they wish to request. It is also necessary to state the time period (start and end date) for which the data is being requested. Applicants are urged to define a start and end date at the beginning/end of either the fiscal or calendar year. This is important as some of the data files are organized either by fiscal or calendar year and, although it is possible to restrict them to either fiscal or calendar year, it is not possible to appropriately filter the files to start at the beginning of a calendar year and end at the end of the fiscal year without the Applicant losing a few months of data.

In the checkboxes provided, please indicate whether all cohorts will require the same data. If NO is selected and a different checklist is required for each cohort please describe in the space provided. An example of this would include a study with two cohorts, each requiring very different fields from MSP. A study could have a cohort of mothers and a cohort of babies and is it possible that WorkSafeBC data is being requested for the mothers, but no WorkSafeBC data is being requested for the babies.

2. External data

Applicants are required to fill in the table in the DAR form specifying with a check mark each data file they wish to request. For external data files that are not listed, please specify the data file name and data source in the space provided under “other”. It is also necessary to state the time period (start and end date) for which the external data is being requested.

Attachment: Attach a copy of any application(s) and approval(s) for use of external data that will be linked to the requested data. Please select the appropriate check box, whether the approval is ATTACHED or, if no external data is being requested for the project, please select NOT APPLICABLE.

Attachment: In addition to the copy of the application(s) and approval(s) for use of external data, it is also necessary to provide a list of fields that have been approved for release from the external data file. If applicable, on this list please identify fields that will be used for linkage only and fields that will be retained for analysis.

3. Researcher-collected data

Include a text description of the researcher-collected data in the space provided in this section. Be sure to include the source of the data, the purpose of collection and the data collection type (survey, questionnaire, focus group, interview, etc.). Please also list the data files included in the data source to facilitate an understanding of the information provided in the table on this page. Please also include any other pertinent details that will give the Data Stewards and the RLU a better understanding of the data source.

In the table provided, enter the name of the data file, describe the data collection type (i.e. survey, questionnaire etc.) and the date range for which the data is available.

Attachment: It is necessary to provide a plain language list of fields that are available in the researcher-collected data file. If applicable, on this list please identify fields that will be used for linkage only and fields that will be retained for analysis.

Informed consent for researcher-collected data

If researcher-collected data or another external data source is to be linked to the data administered by PopData, consent may be required (e.g. when the external data is a survey data set collected by the Applicant). Data Stewards reserve the right to request informed consent of research participants as a requirement under applicable law and/or government policy and procedure. In cases where it is required, the consent form must be included, and needs to include consent to link data for the specified research purposes. This should be the same consent approved by the Research Ethics Board.

If requesting linkage of data from PopData holdings to researcher-collected data, the Applicant will be required to provide written informed consent to use and link the collected data for the specified research purpose(s). Consent documents should explicitly identify proposed linkages and the data involved. It is recommended that the Applicant consult with PopData for suggested wording and consent form guidelines prior to data collection.

Attachment: If YES has been selected and consent has been obtained please provide a copy of a blank consent form and all attachments that will be provided to participants.

If informed consent has NOT been obtained, please select NO. The Applicant will need to provide an explanation and a justification for why consent is impracticable or has been waived. If other methods have been used to obtain consent (e.g., verbal consent), these need to be described.

If no researcher-collected data is being used for the project please select NOT APPLICABLE.

Please be informed that it is a requirement of some Data Stewards (Ministry of Health) to review and approve consent forms prior to data collection. Before commencing any data collection, all consent forms should be submitted to PopData for Data Steward approval.

Please indicate whether or not the consent forms have been pre-approved and indicate the date of the pre-approval. If the consent forms have not been pre-approved, please provide a rationale.

If no pre-approved consent form is required for your project please select NOT APPLICABLE.

SECTION XII: DATA LINKAGE BETWEEN POPULATION DATA BC AND EXTERNAL DATA

This section is for Applicants using or linking to data that is not administered (part of holdings) by PopData and therefore not currently covered by an Information Sharing Agreement between PopData and the Data Provider. We do not have checklists for these data.

In Linkage Table 1 and Linkage Table 2 identify all external data Identifier fields to be used for linkage. Please note these will need to be removed from the extract unless identified as to be retained for analysis.

Linkage Table - 1 Personal Health Number (PHN) or Personal Education Number (PEN)

Please use the table to identify the data source and the availability of a PHN or PEN for linkage. In this table please only identify whether a PHN or PEN is available in the external data source. It is also necessary to provide an estimate of the percentage of individuals in the data that it is anticipated will have a PHN or PEN. *This is important for Population Data BC to plan the linkage that will be required for the project. It also assists Population Data BC in providing a more accurate cost estimate as PHN linkage can be done quickly, while probabilistic linkage can take much longer.* Please also indicate whether it is necessary to retain this field for analysis and if so, provide a strong rationale. **Note:** it is very uncommon for Data Stewards to approve the retention of a PHN or PEN for analysis.

If the external data source has a PHN for 100% of the records and there is a high confidence in the validity of the PHNs, it is not necessary to fill in Linkage Table 2. If PHNs are available for 100% of the records and the Applicant has high confidence in the PHNs, PopData will not use other identifiers such as date of birth and postal code to perform linkage.

Linkage Table 2 - Other identifiers

If necessary, please use this table to identify all identifiers, other than PHN or PEN, that are available to be used for linkage. State the source of the data, the field name (Name, Date of Birth, Postal Code, Sex, etc.) and state whether the field is to be retained for analysis. With a strong rationale, an Applicant may request some identifier fields to be retained.

Request for linkage to occur in a location other than Population Data BC

If linkage is expected to happen outside of PopData, a separate attachment is required to describe how this linkage will occur, any steps that have been, or will be, taken to minimize the privacy risks including timeline for destruction of linkage data. For assistance in creating this linkage strategy please contact the RLU.

Privacy risk considerations

Under the revised BC privacy legislation, some projects may require a completion of a Privacy Impact Assessment.

Please contact the RLU to determine if a Privacy Impact Assessment is required for the project.

SECTION XIII: DATA SECURITY AND ACCESS

1. Use of Secure Research Environment at Population Data BC

Data for approved research projects will be housed the Secure Research Environment (SRE) at PopData unless otherwise authorized. The SRE is a computer server accessible via Virtual Private Network (VPN) using a SecurID token for authentication. The security and privacy policies and processes for the SRE have been audited by an external consultant whose report was approved by all Data Stewards.

The SRE provides Applicants with secure storage and back up of data and access to various software programs for analyzing the data. Visit: www.popdata.bc.ca/dataaccess/process/datadelivery/sre for more information on the SRE.

In some exceptional circumstances Applicants may be granted permission to access the data using another method. To request such permission, Applicants need to provide a written rationale in the space provided on the DAR form, and complete questions 2, 3, 4, 5 and 6 in this section. Please consult the RLU and the provider(s) of the external data prior to completing the DAR.

2. Physical location and security of personal computer

[To be completed by non-SRE users only]

Please indicate the physical location(s) where research data will be used or accessed, including research sites and storage sites (if different). Indicate all general physical security measures in place at each location. Include measures taken to protect workstations, hard copy and source media.

3. Network security and backups

[To be completed by non-SRE users only]

If data will be stored on a network or system to which individuals other than identified project personnel have access, or on a system connected to a public network (the Internet), please indicate, and if appropriate describe the network security measures in place.

4. Personal computer security and backups

[To be completed by non-SRE users only]

If data will be accessed or stored on the hard drive of a personal computer, identify all security measures taken to protect data residing on the PC.

NOTE: Access and storage of record level data on laptop, notebook, handheld devices and other portable devices (e.g. external memory) is NOT ACCEPTABLE without PRIOR WRITTEN AUTHORIZATION from the Data Steward(s). Please contact the RLU at Population Data BC for more information on requesting authorization.

5. Data transfer security

[To be completed by non-SRE users only]

Data and derived information, other than aggregated information such as statistical output, must be transferred using one of following methods: courier; in person by a team member named in the DAR as having access to the data; or secure file transfer as approved by the Data Steward(s). E-mail, regular mail and fax are NOT acceptable transfer methods at any time.

6. Data destruction security

[To be completed by non-SRE users only]

All data and related materials containing data from Population Data BC holdings or linked records generated with data from Population Data BC, such as derived data, duplicated data, analysis tables, working files, backups files, data on server, temporary files, etc. need to be destroyed at the end of a project.

Please note that paper records should be destroyed in a manner that leaves no possibility for reconstruction of information. The accepted method for destroying paper record is cross-cut shredding.

For more detailed information, please refer to the PopData *Project closure guidelines and data destruction form*. Written notice of data destruction is to be provided, as outlined in the Research Agreement and above guidelines document.

7. Declaration

In order to confirm that the Applicant, and PI if applicable, have read and understood the above section on Data Security and Access, please select the check box.

SECTION XIV: SIGNATURE AND DECLARATION

If the Applicant is a different person than the PI, please select the check box YES. If YES is selected, both individuals must sign the form below with a witness present. **Note:** For a student application, the Applicant will be the student and the PI will be the supervisor.

This section completes the application and should be signed at the point when the DAR has been finalised and confirmed by the RLU that it is ready for submission to the Data Steward(s).

IN CLOSING

Project communications

Once the DAR has been received by PopData, the project will be issued a project number for tracking purposes. The assignment of the tracking number does not necessarily mean the review process has been activated. While every DAR will receive a tracking number, not every DAR will be approved.

Please use the title that appears on the DAR and the PopData-assigned project number on all future correspondence with PopData.

As PopData facilitates communications, and additional requests as required by the Data Steward(s) the RLU staff need to be copied on all direct communications/consultation with relevant Data Steward(s).

Questions and help

Population Data BC's Researcher Liaison staff are available to help researchers with the DAR process; that said, staff time is a finite resource. **Only complete applications will be reviewed by Researcher Liaison Unit staff. Applications received that are missing required documents, or do not meet a certain standard of consistency (i.e. consistency between the DAR and ethics application) will be returned to the Applicant and will not be processed until the application is re-submitted as a complete package.**

PopData is working to move many of the support-related functions to the web in order to maintain high levels of support for applications. Prior to contacting the RLU, Applicants are urged to check the PopData website to answer questions. If an Applicant cannot find the information needed on the PopData website, they should then contact the RLU.

SECTION I: APPLICATION DETAILS

USE THIS APPLICATION TO REQUEST DATA ADMINISTERED BY POPULATION DATA BC.

NOTE: Population Data BC administers data and coordinates applications for research data linkages; however, the Data Steward of the public body (e.g. the Ministry of Health, WorkSafeBC) that has custody or control over the data holds the legal authority for approving the disclosure of the data for a specific research purpose.

APPLICANT

PRINCIPAL INVESTIGATOR (IF DIFFERENT FROM APPLICANT)

PROJECT TITLE

IF THIS IS A STUDENT REQUEST TO ACCESS EXISTING APPLICANT DATA, PLEASE PROVIDE THE APPROVED PROJECT NUMBER

FOR POPULATION DATA BC (POPDATA) USE ONLY

PopData Project Number	
Date PopData Submitted to Data Stewards:	DAR Version (e.g. V-1 2012-01-01):
FOR RESUBMISSIONS ONLY:	
Resubmission Date:	Resubmission Version (e.g. V-2 2012-03-01):

FOR BC MINISTRY OF HEALTH USE ONLY

Ministry Project Number:	
Date Criteria Check Completed:	DAR Category:
3-Month Review Commitment Start Date:	3-Month Review Commitment End Date:

SECTION II: APPLICATION SUBMISSION PROCESS

- Fill out the application to the best of your ability using the DAR Manual located on Population Data BC's website, www.popdata.bc.ca
- Collaborate with the Researcher Liaison Unit to complete your Study Population Description and discuss linkages.
- Submit a completed DAR, including *ALL* required attachments electronically to the Researcher Liaison Unit at Population Data BC: rlu@popdata.bc.ca
- The completeness of the application will be assessed by the Researcher Liaison Unit at Population Data BC; only complete applications will be submitted for Data Steward Review.
- Population Data BC submits applications to the relevant Data Stewards on behalf of the Researcher.
- If this Data Access Request is approved by the applicable Data Steward(s), this application becomes a schedule to a legally enforceable Research Agreement.
- The Applicant and Principal Investigator (PI), if different from the Applicant, must sign the Research Agreement before data are released, as required by the BC Freedom of Information and Protection of Privacy Act (FIPPA), section 35(1)(d). All study team members are required to sign a confidentiality pledge as a schedule to the Research Agreement.

The following will help to facilitate the review of your DAR

- Become familiar with all material outlining access requirements, data holdings, and privacy considerations on Population Data BC's website www.popdata.bc.ca
- Questions about the application process or any part of your application may be directed to the Researcher Liaison Unit at Population Data BC: rlu@popdata.bc.ca
- Please ensure the following information is consistent on *ALL* project documentation including the DAR, ethics applications and certificates, funding applications, external data applications and agreements, letters of support and any other project documentation.
 - Project Title
 - Research Team
 - Research Objectives
 - Study Population Description
 - Data Linkages
 - All dates and date ranges

SECTION III: FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (FIPPA)

Information collected on these forms is governed by FIPPA. The collection of personal information on this form by the public body holding the data requested is authorized under section 26(c) of FIPPA. The personal information that is collected, such as name, address, phone number and any other personal information is required to process and adjudicate the application and to contact you to discuss any issue relevant to the application. Do not include the personal information of others unless you have their authorization (i.e., consent) to do so.

Questions regarding the collection of personal information may be directed to the public body in question or, to assist in contacting the public body, to:

Privacy Officer, Population Data BC
201-2206 East Mall
Vancouver, BC V6T 1Z3

Phone: 604-822-6514
Fax: 604-822-5690
privacy@popdata.bc.ca

CONSENT FOR POPULATION DATA BC TO PUBLISH PROJECT INFORMATION

NOTE: Population Data BC would like the opportunity to publish details about successful applicants, including on the Population Data BC website. Please indicate below your consent for use of all or part of the described information collected on this application.

I give Population Data BC permission to publish the following project information upon project approval:

- ☐ Applicant and PI Name
- ☐ Institution
- ☐ Project title
- ☐ Funding agency
- ☐ Research objectives
- ☐ Approved data sets
- ☐ Publication information
- ☐ **All of the above**
- ☐ **None of the above**

SECTION IV: PREVIOUSLY APPROVED DATA REQUESTS RELEVANT TO THIS APPLICATION

Is the request related to a previously approved data release from PharmaNet or the Ministry of Health (including holdings at Population Data BC)? ☐ YES ☐ NO

If **YES**, please provide the following:

PharmaNet Data Request (DSC) File Number:

Ministry of Health Data Request (DAR) Project Number(s):

Explanation of relationship to previously approved data request:

SECTION V: REQUEST TO CONTACT

Does this project require the use of data from the Ministry of Health (including holdings at Population Data BC) or a Health Authority or PharmaNet to contact individuals to request their participation in health research?

☐ YES ☐ NO



ATTACHMENTS

If **YES**, please complete and attach the “Request to Contact Potential Study Participants” form or attach approval letter if permission to contact has been authorized.

SECTION VI: REQUIRED DOCUMENTATION CHECKLIST

Electronic copies of all required supporting documents must be included with the application.

CHECK APPLICABLE BOXES

REQUIRED DOCUMENTATION: CONFIRM ATTACHMENT OF DOCUMENTS LISTED BELOW	SECTION
<input type="checkbox"/> Peer Review: Copy of funding application or contract proposal submitted	VIII
<input type="checkbox"/> Peer Review: Final funding letter or contract (removing financial information)	VIII
<input type="checkbox"/> Ethical Review: Copy of application for ethics review, and all supporting documents	VIII
<input type="checkbox"/> Ethical Review: Ethics Certificate	VIII
<input type="checkbox"/> All applicable data field checklists	XI

IF NOT PEER REVIEWED:	SECTION
<input type="checkbox"/> Supervisory letter of review OR	VIII
<input type="checkbox"/> Applicant CV	VIII

ADDITIONAL DOCUMENTATION AS APPLICABLE	SECTION
<input type="checkbox"/> Request to contact potential study participants form	V
<input type="checkbox"/> Please attach details of the Applicant, and/or Applicant's relations pertaining to conflict of interest	VIII
<input type="checkbox"/> Authorization for use of the data that will be linked to data administered by Population Data BC: e.g., agreement with or letter from external data source including application, consent documents	XI
<input type="checkbox"/> Plain-language description of all fields external to Population Data BC to be retained for analysis (external data)	XI
<input type="checkbox"/> Plain-language description of all fields external to Population Data BC to be retained for analysis (researcher collected data fields)	XI
<input type="checkbox"/> Informed consent form and any attachments provided to participants, as approved by a ethics review board	XI
<input type="checkbox"/> Rationale as to why linkage cannot be performed by Population Data BC describing steps taken to minimize the privacy risks	XII
<input type="checkbox"/> Description of all measures taken to minimize the privacy risks of any proposed linkage, and Privacy Impact Assessment	XII

SECTION VII: APPLICANT AND RESEARCH TEAM INFORMATION

This section outlining the research team should match the approved Research Ethics Board Application for the project exactly.

APPLICANT

The Applicant must be a person who is listed as Principal Investigator or Co-investigator in the Ethics Board Approval (or official waiver process) from an accredited Ethics Review Board (REB), such as at a University or Hospital. If the project is a thesis or dissertation, the Applicant must be the student.

LAST NAME		FIRST NAME		TITLE	
STREET ADDRESS		CITY	PROV	COUNTRY	POSTAL CODE
PHONE	FAX	EMAIL			
POSITION		INSTITUTION NAME			

INSTITUTION ADDRESS (if different from Applicant address)

STREET ADDRESS		CITY	PROV	COUNTRY	POSTAL CODE
PHONE	FAX	EMAIL			

PRINCIPAL INVESTIGATOR (if different from Applicant)

The Principal Investigator is an individual who either has a faculty appointment (Clinical Assistant Professor, Clinical Associate Professor, Clinical Professor, Assistant Professor, Associate Professor, Professor or BCCA Investigator) OR is deemed a PI by an affiliated institution or by a Dean. This individual bears the overall responsibility for the conduct of the study, including the activities of co-investigators, who are assumed to be acting under the delegated authority of the PI, and is required to act within the requirements of the Tri-Council Policy Statement (TCPS).

The Principal Investigator should be the same individual listed in the ethics board approval as well as in approvals for use of other data. If this is not feasible, please discuss with the Researcher Liaison Unit at Population Data BC.

LAST NAME		FIRST NAME		TITLE	
STREET ADDRESS		CITY	PROV	COUNTRY	POSTAL CODE
PHONE	FAX	EMAIL			
POSITION		INSTITUTION NAME			

PROJECT COORDINATOR / MANAGER (primary contact person for correspondence, etc.)

LAST NAME		FIRST NAME		TITLE	
STREET ADDRESS		CITY	PROV	COUNTRY	POSTAL CODE
PHONE	FAX	EMAIL			
POSITION		INSTITUTION NAME			

CO-INVESTIGATORS

NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION

THESIS/DISSERTATION SUPERVISOR(S) (if data are to be used for a thesis or dissertation)

LAST NAME		FIRST NAME		TITLE	
STREET ADDRESS		CITY	PROV	COUNTRY	POSTAL CODE
PHONE	FAX	EMAIL			
POSITION		INSTITUTION NAME			

LAST NAME		FIRST NAME		TITLE	
STREET ADDRESS		CITY	PROV	COUNTRY	POSTAL CODE
PHONE	FAX	EMAIL			
POSITION		INSTITUTION NAME			

LAST NAME		FIRST NAME		TITLE	
STREET ADDRESS		CITY	PROV	COUNTRY	POSTAL CODE
PHONE	FAX	EMAIL			
POSITION		INSTITUTION NAME			

AUTHORIZED USERS - PERSONS WHO WILL HAVE ACCESS TO THE DATA

Identify all individuals who will have access to the requested data AT ANY TIME. Please include any of the Applicant, Principal Investigator, Project Coordinator/Manager or Co-Investigators and/or Thesis/Dissertation Supervisors on this list if they will be accessing the research extract. Attach separate sheet if necessary. A signed pledge of confidentiality will be required of each identified individual before data are released.

NAME	POSITION	INSTITUTION	EMAIL ADDRESS
NAME	POSITION	INSTITUTION	EMAIL ADDRESS
NAME	POSITION	INSTITUTION	EMAIL ADDRESS
NAME	POSITION	INSTITUTION	EMAIL ADDRESS
NAME	POSITION	INSTITUTION	EMAIL ADDRESS
NAME	POSITION	INSTITUTION	EMAIL ADDRESS
NAME	POSITION	INSTITUTION	EMAIL ADDRESS
NAME	POSITION	INSTITUTION	EMAIL ADDRESS
NAME	POSITION	INSTITUTION	EMAIL ADDRESS
NAME	POSITION	INSTITUTION	EMAIL ADDRESS
NAME	POSITION	INSTITUTION	EMAIL ADDRESS
NAME	POSITION	INSTITUTION	EMAIL ADDRESS
NAME	POSITION	INSTITUTION	EMAIL ADDRESS
NAME	POSITION	INSTITUTION	EMAIL ADDRESS
NAME	POSITION	INSTITUTION	EMAIL ADDRESS
NAME	POSITION	INSTITUTION	EMAIL ADDRESS

1. WHO IS FUNDING YOUR RESEARCH PROJECT?

☐ Canadian Institutes of Health Research

☐ Canadian Health Services Research Foundation

☐ Social Sciences and Humanities Research Council Expiry date: _____

☐ Michael Smith Foundation for Health Research Expiry date: _____

☐ WorkSafeBC

☐ Other funding organization (please specify): _____ Expiry date: _____

☐ Other funding organization (please specify): _____ Expiry date: _____

☐ Other funding organization (please specify): _____

Expiry date: _____

☐ In-kind donations (source): _____

--

--

- ☐ Funds provided by private industry
(describe source(s)):

Expiry date: _____

CONFLICT OF INTEREST



ATTACHMENTS

If the Applicant, and/or Applicant's spouse, domestic partner or child has an association or connection of any kind, whether financial or non-financial, with any sponsor of the project or the manufacturer or owner of any drug, device, program, or method being evaluated in the project, please attach details.

Examples of financial interests include ownership of stocks, bonds, options, patent or royalty interests, receipt of consulting, honoraria, or speaking fees, salary, subject accrual rewards or penalties, loans, lectureships, memberships on boards of directors or scientific advisory boards. Examples of non-financial relationships include previous research collaborations, student/teacher relationships, other personal or professional relationships, professional differences, or any other connection that might lead to the perception of influence on the study.

- ☐ ATTACHED ☐ NOT APPLICABLE

2. EXTERNAL PEER REVIEW OF YOUR RESEARCH PROJECT

- ☐ My project has been reviewed by an external peer committee, such as a grant funding agency



Attach a copy of the following documents:

- a) Project description from application [for Population Data BC use only]
- b) Final funding letter

- ☐ My project is a thesis or dissertation and has been reviewed by my supervisory committee



Attach a letter from the supervisory committee indicating that the proposal has been approved

- ☐ My project has not been peer reviewed



Attach a complete CV for the Applicant

3. ETHICAL REVIEW OF YOUR RESEARCH PROJECT



Attach a copy of current ethics application and approval

Organization	Certificate Number	Expiry Date

☐ My project has not been submitted for ethical review (provide explanation)

IF THE PROJECT HAS NOT BEEN APPROVED OR SUBMITTED FOR REVIEW BY AN ACCEPTABLE* ETHICS REVIEW COMMITTEE, the Data Steward(s) may refuse to consider the application.

***NOTE:** Only non-profit ethics review committees, such as those at universities, are acceptable. The Data Steward reserves the right to decide the acceptability of ethics review committees in their sole and absolute discretion.

SECTION IX: RESEARCH PROJECT DESCRIPTION

PROJECT TITLE

TITLE DIFFERENCE

If the title above differs from funding approvals, ethics review documentation or external data source approval, indicate the reason for the discrepancy.

PUBLIC INTEREST VALUE/PUBLIC BENEFIT OF PROJECT

SMALL CELL SIZE

Please describe measures that will be taken to protect confidentiality (identification of an individual) during analysis and in any publication or distribution of results when dealing with small cell size.

DESCRIPTION OF THE PROJECT

Describe the project including its purpose and background. Include an introduction to the project and if relevant, its relationship to any other program of research (e.g. phased or existing studies)

RESEARCH OBJECTIVES: RESEARCH QUESTIONS AND HYPOTHESES

Please 1) List research questions and 2) Identify hypotheses

METHODOLOGY

Summarize the study design and methodology.

ACHIEVING RESEARCH OBJECTIVES

Describe how the linkage for this study and data requested from each data file, including external data sources, are necessary to achieve your research objectives (e.g. MSP, DAD, etc.).

SECTION X: DEFINING YOUR STUDY POPULATION

READ THIS SECTION CAREFULLY.

The Applicant must collaborate with Population Data BC to complete this section of the DAR.

A study population is the group of subjects that a researcher wants to include in their analyses. The study population may include multiple cohorts as well as one or more comparison group(s). Applicants must define their study population in text and use as much detail as possible. These details should include all information that will assist Population Data BC in creating the study population Technical Definition.

NOTE: The variables described in the study population definition are not necessarily the variables that will be provided in the research extract. The years of data and variables required for the research extract are listed in the checklists in Section XI.

IMPORTANT: A clear, explicit rationale is required for inclusion of all proposed individuals in the study population. The rationale must be clearly related to the research question(s) and methods.

Applicants are advised that any changes to the study population after approval may require an amendment, further review and adjudication by the Data Steward(s) and will incur a fee in addition to any previous estimates or costs paid.

1. WHO IS CREATING THE STUDY POPULATION

a) The study population will be defined using data from the following sources, check all that apply:

- ☐ Population Data BC
- ☐ PharmaNet
- ☐ Health Information Bank
- ☐ External data → ☐ Check if more than one external data set
- ☐ Researcher-collected data → ☐ Check if more than one researcher-collected data set

b) Applicants who want to use data from **outside** Population Data BC to define the project-specific study population are required to complete the tables **LINKAGE TABLE 1** and/or **LINKAGE TABLE 2** in the Section XII DATA LINKAGE BETWEEN POPULATION DATA BC AND EXTERNAL DATA.

REMEMBER: Applicants must also complete and submit any necessary protocols for requesting and linking external data. Copies of applications and final approvals to use and link data from an external source must be submitted as part of the application package.

2. TEXT DESCRIPTION

Please describe the Study Population, and as relevant include description of study cohort and study control or comparison group:

Provide a text description of your study population. This description should include as much detail as possible, such as health condition(s), age groups, date ranges or geographic areas, specific databases used to create the study population, as well as specifications for sampling or matching, as required for the comparison group(s). Include specific exclusion criteria if relevant. If known, please include an estimate of the anticipated size of the cohort(s) to facilitate an accurate estimate of data extract costs.


3. RATIONALE FOR STUDY POPULATION IN RELATION TO RESEARCH OBJECTIVES

Applicants must clearly illustrate how the study population is designed to meet the stated research objectives. If requesting a population-based cohort please explain why your research objectives cannot be met by sampling or by using a sub-set of the population.

SECTION XI: DATABASES USED FOR EXTRACT

IMPORTANT: Applicants may request data to the end of the current year only (fiscal or calendar year).

NEXT STEP

 Download and complete the appropriate data field checklists at <http://www.popdata.bc.ca/dataaccess/documentcentre>

These forms will become part of the legal agreement between the Applicant and the applicable public body.

1. INTERNAL DATA (housed at Population Data BC)

DATA FILES AND YEARS OF DATA REQUESTED

Data File	From Date (YYYY/MM/DD)	To Date (YYYY/MM/DD)
Health Care and Health Services Data		
<input type="checkbox"/> Medical Services Plan Payment Information (MSP) File April 1, 1985 onwards		
<input type="checkbox"/> Home and Community Care January 1, 1990 onwards		
Discharge Abstracts Database April 1, 1985 onwards		
<input type="checkbox"/> Mental Health Services April 1, 1986 onwards		
<input type="checkbox"/> PharmaCare January 1, 1985 onwards		
BC Cancer Agency January 1, 1985 onwards		
Population and Demographic Data		
<input type="checkbox"/> Consolidation File January 1, 1986 onwards		
Vital Statistics Births January 1, 1985 onwards		
Vital Statistics Deaths January 1, 1985 onwards		
Vital Statistics Marriages January 1, 1985 onwards		
Vital Statistics Stillbirths January 1, 1985 onwards		
<input type="checkbox"/> Statistics Canada Income Band 1992, 2002, 2006		
<input type="checkbox"/> Citizenship and Immigration Canada (CIC) January 1, 1985 onwards		

Data File	From Date (YYYY/MM/DD)	To Date (YYYY/MM/DD)
Occupational Data		
<input type="checkbox"/> WorkSafeBC Files January 1, 1987 onwards unless otherwise noted		
Early Childhood Data		
Early Development Instrument (EDI) 2000 onwards		
<input type="checkbox"/> Middle Years Development Instrument (MDI) 2010 onwards		
Spatial Data		
Integrated Cadastral Information Society (ICIS)		
Other Data		
<input type="checkbox"/> Other (specify):		
<input type="checkbox"/> Other (specify):		

Do all cohorts require the same data (e.g. the same data files, data fields, or the same time period)?

☐ YES

☐ NO

If NO, please provide a brief description of the differences and ensure separate checklists are provided for each

(e.g. a study with two cohorts each requiring very different fields from MSP)

2. EXTERNAL DATA

External data is data from other organizations. It is not held at Population Data BC and not collected by the researcher.

DATA FILES AND YEARS OF DATA REQUESTED

Data File	From Date (YYYY/MM/DD)	To Date (YYYY/MM/DD)
<input type="checkbox"/> PharmaNet ClaimHist		
<input type="checkbox"/> PharmaNet MedHist		
<input type="checkbox"/> BC Perinatal Database		
<input type="checkbox"/> Medical Charts (Source:_____)		
OTHER:		



ATTACHMENT

Attach a copy of any application(s) and approval(s) for use of external data that will be linked to the requested data.

☐ ATTACHED ☐ NOT APPLICABLE

NOTE: The applications / approvals must fully disclose ALL proposed linkages.



ATTACHMENT

Attach a list and plain-language description of ALL External Data fields to be retained for analysis. The Data Steward(s) adjudicate based upon the entire linkage, and not only for the data under their authority or the use of specific identifiers.

☐ ATTACHED ☐ NOT APPLICABLE

3. RESEARCHER COLLECTED DATA

Please include a text description of the researcher collected data in the space provided below. Please include the source of the data, purpose of collection and the data collection type (e.g. survey/ questionnaire, focus group, interview).

Please identify the availability (dates) of the researcher collected data below:

Data File	Data Collection Type	From Date (YYYY/MM/DD)	To Date (YYYY/MM/DD)



ATTACHMENT

Attach a list and plain-language description of ALL researcher collected data fields to be retained for analysis. The Data Steward(s) adjudicate based upon the entire linkage, and not only for the data under their authority or the use of specific identifiers.

☐ ATTACHED ☐ NOT APPLICABLE

INFORMED CONSENT FOR RESEARCHER COLLECTED DATA

Informed consent is required for researcher collected data. Data Stewards **reserve the right** to request Informed Consent of research participants as a requirement under applicable law and /or government policy and procedure.

If you are requesting to link data from Population Data BC to researcher collected data, confirm if you have obtained, or will obtain, written, informed consent to use and link the collected data for the specified research purpose(s) from research participants. Has informed consent been obtained?

☐ YES ☐ NO ☐ NOT APPLICABLE



ATTACHMENT (If YES)

If **YES**, attach a blank copy of the informed consent and any attachments provided to participants, as approved by the research ethics board. Consent documents should explicitly identify proposed linkages and the data involved. Consult with Population Data BC for suggested wording.

If **NO**, provide rationale. If other methods have been used to obtain consent to access this information (e.g. verbal consent), please describe:

Has this consent form been pre-approved by the Data Stewards prior to data collection?

☐ YES ☐ NO ☐ NOT APPLICABLE

If **YES**, List Data Stewards _____
and Date of Approval _____

If **NO**, provide rationale.

SECTION XII: DATA LINKAGE BETWEEN POPULATION DATA BC AND EXTERNAL DATA

Many Applicants request to use data from **outside** Population Data BC to define the study population and/or request a research extract. Population Data BC requires linkage variables to link the study population to the research data for these projects. More specifically, Population Data BC requires the Applicant to indicate whether personal health numbers (PHNs) or personal education numbers (PENs) are available for the external data, or if other identifiers are required to facilitate linkage. Applicants should be aware that regardless of the linking variables used, a 100% match of any study population to data at Population Data BC is not possible.

Identify below all data sources and identifier fields that you propose to use **for linkage**. Unless otherwise stated, it is expected that linkage will occur at Population Data BC.

As stipulated in the Research Agreement, a researcher can request some identifier fields to be retained for analysis. Please identify and provide a detailed rationale for such a request in the space provided.

LINKAGE TABLE 1 - Personal Health Number (PHN) or Personal Education Number (PEN):

Data Source	Field Name (PHN/PEN)	% Availability (e.g. estimated percentage of available PHNs)	Retain for Analysis (Yes/No)	Justification if Retaining for Analysis

LINKAGE TABLE 2 - Other Identifiers:

Data Source	Field Name	Retain for Analysis (Yes/No)	Justification if Retaining for Analysis

REQUEST FOR LINKAGE TO OCCUR IN A LOCATION OTHER THAN POPULATION DATA BC

☐ YES ☐ NO



ATTACHMENT (If YES)

If **YES**, provide a rationale as to why linkage cannot be performed by Population Data BC and describe any steps that have been, or will be, taken to minimize the privacy risks of the proposed linkage at all stages. In particular, ensure the timeline for proposed removal and destruction of data used only for linkage is included.

PRIVACY RISK CONSIDERATIONS

Contact Population Data BC at rlu@popdata.bc.ca to determine if a Privacy Impact Assessment is required for your project.

If applicable, a Privacy Impact Assessment is included.

☐ YES ☐ NOT APPLICABLE



ATTACHMENT (If YES)

If **YES**, provide the Privacy Impact Assessment.

SECTION XIII: DATA SECURITY AND ACCESS

1. USE OF SECURE RESEARCH ENVIRONMENT AT POPULATION DATA BC

Research Extracts will be housed on the Secure Research Environment at Population Data BC, unless otherwise authorized. The Secure Research Environment is a central server to which secure remote access, storage and back-ups are provided to the project-specific Research Extract, and for the provision of data analysis software.

Please see my.popdata.bc.ca/sre for more information including a list of the software available.

Will you be requesting access to the Secure Research Environment at Population Data BC?

☐ YES ☐ NO

If **YES**, skip to item 7 in this section

If **NO**, provide rationale and complete items 2 through 4 in this section. In cases where external data are being linked outside of Population Data BC, explain measures taken to prevent re-linking of Research Extract with original external data.

2. PHYSICAL LOCATION AND SECURITY OF DATA

Indicate the physical locations(s) where research data will be used or accessed, including research sites, and storage sites (if different). Indicate all general physical security measures in place at each location. Include measures taken to protect workstations, hard copy and source media.

LOCATION 1

SITE		ORGANIZATION NAME		
STREET ADDRESS				
CITY		PROV	COUNTRY	POSTAL CODE
PHYSICAL SECURITY METHODS				
<input type="checkbox"/> LOCKED FILE CABINET <input type="checkbox"/> DOOR KEYPAD <input type="checkbox"/> OTHER (SPECIFY):				

LOCATION 2

SITE		ORGANIZATION NAME			
STREET ADDRESS					
CITY			PROV	COUNTRY	POSTAL CODE
PHYSICAL SECURITY METHODS <input type="checkbox"/> LOCKED FILE CABINET <input type="checkbox"/> DOOR KEYPAD <input type="checkbox"/> OTHER (SPECIFY):					

NOTE: All physical locations housing data must be locked, except when an individual authorized to access the data is present.

3. NETWORK SECURITY AND BACKUPS

If data will be stored on a network or system to which individuals other than identified project personnel have access, or on a system connected to a public network (the internet), indicate and describe the network security measures in place.

Location 1

- ☐ Firewall
- ☐ Password changed every_____ days
- ☐ Password rules (minimum length, complexity)
- ☐ Drives or folders with access restricted to specific research group
- ☐ File encryption
- ☐ Other:_____
- ☐ Security audit:_____
- ☐ Access tracking:_____

Describe how, and from where, any regular maintenance and backups of your network are conducted, where backup material is stored, and backup retention schedule.

Location 2

- ☐ Firewall
- ☐ Password changed every _____ days
- ☐ Password rules (minimum length, complexity)
- ☐ Drives or folders with access restricted to specific research group
- ☐ File encryption
- ☐ Other: _____
- ☐ Security audit: _____
- ☐ Access tracking: _____

Describe how, and from where, any regular maintenance and backups of your network are conducted, where backup material is stored, and backup retention schedule.

4. PERSONAL COMPUTER SECURITY AND BACKUPS

If data will be accessed or stored on the hard drive of a personal computer, identify all security measures taken to protect data residing on the PC.

- ☐ Electronic locking system
- ☐ Encryption
- ☐ Logon password
- ☐ Removable drives
- ☐ Individual file or folder passwords
- ☐ Physical attachment to floor or object
- ☐ Software firewall (describe): _____
- ☐ Antivirus (describe): _____
- ☐ Antispyware or adware (describe): _____
- ☐ Other (describe): _____

NOTE: Storage of data on laptops, notebooks, handheld devices and other portable devices (e.g. external memory) is not permitted. Access from portable devices is allowed only through the Secure Research Environment, and only under security conditions specified for that environment.

5. DATA TRANSFER SECURITY

Data and derived information, other than aggregated information such as statistical output, must be transferred by a secure file transfer as approved by the applicable Data Steward(s). If this method is not possible, then an encrypted or password protected media must be used meeting the appropriate transfer protocols for the relevant Public Body; or transferred in person by someone named above as having access to the data. Email, regular mail, and fax are NOT acceptable transfer methods at any time.

6. DATA DESTRUCTION SECURITY IF NOT USING SECURE RESEARCH ENVIRONMENT

Upon project completion or cessation, the data and any copies must be destroyed using a method of destruction that is equivalent or superior to the standard established by the BC government and must follow the Population Data BC project closure guidelines. Contact rlu@popdata.bc.ca for project closure and data destruction procedures.

7. DECLARATION

- ☐ The Applicant and Principal Investigator, if different from Applicant, declare the above section on data security and access requirements has been read and understood.

SECTION XIV: SIGNATURE AND DECLARATION

Is the Applicant different from and Principal Investigator?

☐ YES ☐ NO

If **YES**, the Applicant and Principal Investigator must sign below.

NOTE: Once this DAR is approved, the Applicant, as well as the Principal Investigator if applicable, will need to enter into a Research Agreement. This application will become a schedule to the Research Agreement.

APPLICANT

I declare that all information provided in this application is complete and correct.

Applicant Signature

Print Name

Date Signed

Witness Signature

Print Name

Date Signed

PRINCIPAL INVESTIGATOR

I declare that all information provided in this application is complete and correct.

Principal Investigator Signature
[if different from Applicant]

Print Name

Date Signed

Witness Signature

Print Name

Date Signed

Data Retention Extension Application Form

Date of Submission:

Project Information

Project Number:

Project Title:

Principal Investigator/Applicant:

Address/ Phone/ Email:

Current Data Retention Date:

Current Ethics Approval:

Review Body:

Certificate Number:

Expiry Date:

Current Funding Source:

Funding Expiry Date:

Approved Data Request: *List all approved data files and date range*

Current Approved Study Population Description:

Please enter the study population description approved on your DAR, please also include any additions to this description that may have been approved under a past amendment.

Data Storage: ☐ Population Data BC Secure Research Environment
☐ Other: Rationale:

List Team Members with Data Access:

Data Retention Data Extension Request (1 year)

Rationale:

Insert rationale

Expected project End Date:

New Data Retention Date Requested: *to be completed by PopData*

Project Title	Applies to Subpopulation(s)
----------------------	------------------------------------

Date Range	yyyy/mm/dd	to	yyyy/mm/dd
Other date range criteria:			

Consolidation File (January 1, 1986 onwards)	
<p>Derived from Medical Services Plan Registration and Premium Billing (R&PB) snapshot files, by fiscal year. The Consolidation File reflects work done to clean and consolidate the Registration and Premium Billing files. Demographic and geographic data fields are extracted from the Consolidation File by default. If you wish to request demographic and/or geographic information from a specific data file other than the Consolidation File, please contact Population Data BC.</p> <p>This file also contains two simplified registration summary fields suitable for most needs: start day registered in year (point in the year that their registration started) and total days registered during the year. Exact enrollment and cancellation dates are available, but should be requested in a covering letter.</p>	
DEMOGRAPHIC FIELDS	
<input type="checkbox"/>	Year of birth
<input type="checkbox"/>	Month of birth
<input type="checkbox"/>	Day of birth – Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Sex
GEOGRAPHIC FIELDS	
<input type="checkbox"/>	Neighbourhood income (SES) quintile / decile
<input type="checkbox"/>	Health authority (HA)
<input type="checkbox"/>	Health service delivery area (HSDA)
<input type="checkbox"/>	Local health area (LHA) – Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Census division (CD)
<input type="checkbox"/>	Census subdivision (CSD) Note: this field must be combined with census division in order to uniquely identify a CSD. – Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Census metropolitan area / census agglomeration area(CMA/CA)
<input type="checkbox"/>	Census tract (CT) Note: this field must be combined with a CMA/CA code to uniquely identify a CT. – Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Dissemination area (DA) – Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	First three characters of the postal code (forward sortation area)

<input type="checkbox"/>	6-digit postal code – Research rationale describing why this field is required must be supplied before it will be considered for release:
REGISTRATION FIELDS	
<input type="checkbox"/>	Start day registered in year (point in the year registration started)
<input type="checkbox"/>	Total days registered in year
FIELDS FOR GROUPING ECONOMIC FAMILIES	
<input type="checkbox"/>	MSP contract number Replaced by project-specific identification number
<input type="checkbox"/>	Contract holder flag

Project Title	Applies Subpopulation (s)
----------------------	----------------------------------

Date Range	yyyy/mm/dd	to	yyyy/mm/dd
-------------------	------------	----	------------

Other date range criteria:

Discharge Abstracts Database (Hospital Separations) (April 1, 1985 onwards)	
Includes discharges, transfers and deaths of in-patients from acute care hospitals in BC, including day surgeries. Fields are available in all years unless otherwise noted. <i>Note: Files are grouped into fiscal years by separation date, not the date of admission.</i>	
<input type="checkbox"/>	BC hospital number – Replaced by project-specific identification number
OR	
<input type="checkbox"/>	BC hospital number (unencrypted) – Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Level of care
<input type="checkbox"/>	Admission date
<input type="checkbox"/>	Admission time (hour only until 2001/02) Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Discharge (separation) date
<input type="checkbox"/>	Discharge (separation) time (hour only until 2001/02) Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Admit category
<input type="checkbox"/>	Ambulance code
<input type="checkbox"/>	Ambulance flag 85/86 – 00/01
<input type="checkbox"/>	Readmission code 01/02 onward
<input type="checkbox"/>	Entry code 90/91 onward
<input type="checkbox"/>	Exit code 85/86 – 00/01
<input type="checkbox"/>	Autopsy 91/92 – 00/01
<input type="checkbox"/>	Coroner 91/92 – 00/01
<input type="checkbox"/>	Operative death code 91/92 – 00/01
<input type="checkbox"/>	Supplemental death code 91/92 – 00/01
<input type="checkbox"/>	Discharge (separation) disposition 01/02 onward
<input type="checkbox"/>	Death in OR indicator 01/02 onward
<input type="checkbox"/>	Death in special care unit (SCU) indicator 01/02 onward
<input type="checkbox"/>	Long term care assessment code 85/86 – 95/96

<input type="checkbox"/>	Long term care assessment for DPU code	85/86 – 95/96
<input type="checkbox"/>	Acute/rehab days	
<input type="checkbox"/>	Alternate level of care (ALC) length of stay	
<input type="checkbox"/>	Chronic behaviour disorder (CBD) unit days	
<input type="checkbox"/>	Coronary intensive care nursing unit days	
<input type="checkbox"/>	Discharge planning unit (DPU) days	85/86 – 00/01
<input type="checkbox"/>	Intensive care unit (ICU) days	
<input type="checkbox"/>	Rehabilitation days	
<input type="checkbox"/>	Total length of stay	
<input type="checkbox"/>	Length of stay group 1	85/86 – 06/07
<input type="checkbox"/>	Length of stay group 2	85/86 – 06/07
<input type="checkbox"/>	Hospital size	90/91 – 06/07
<input type="checkbox"/>	BC hospital number transferred from – Replaced by project-specific identification number	
	OR	
<input type="checkbox"/>	BC hospital number transferred from (unencrypted) – Research rationale describing why this field is required must be supplied before it will be considered for release:	
<input type="checkbox"/>	BC hospital number transferred to – Replaced by project-specific identification number	
	OR	
<input type="checkbox"/>	BC hospital number transferred to (unencrypted) – Research rationale describing why this field is required must be supplied before it will be considered for release:	
<input type="checkbox"/>	Level from	85/86 to 00/01
<input type="checkbox"/>	Level to	85/86 to 00/01
<input type="checkbox"/>	BC care level from	01/02 - onward
<input type="checkbox"/>	BC care level to	01/02 - onward
<input type="checkbox"/>	Service transfer service (1 to 3)	91/92 onward
<input type="checkbox"/>	Service transfer days (1 to 3)	91/92 onward
<input type="checkbox"/>	Main patient service	
<input type="checkbox"/>	Patient service group	90/91 – 06/07
<input type="checkbox"/>	Provider 1 (most responsible physician) Replaced by project-specific identification number	
<input type="checkbox"/>	Provider 1 (most responsible physician) service [Note: Not the same as registered specialty]	
<input type="checkbox"/>	Diagnosis (ICD9 codes) (Note: - must be used with diagnosis type, below)	max. 16 in 85/86 – 00/01; 25 in 01/02 – 06/07
<input type="checkbox"/>	Diagnosis (ICD10-CA codes) (Note: - must be used with diagnosis type, below)	max. of 25 codes in 01/02 onward
<input type="checkbox"/>	Diagnosis type	max. of 16 in 85/86 – 00/01; 25 in 01/02 onward
<input type="checkbox"/>	Diagnosis class	85/86 – 06/07

<input type="checkbox"/>	Diagnostic short list (based on ICD9 coding)	90/91 – 06/07
<input type="checkbox"/>	Pre-admit co-morbidity (diagnosis 2)	85/86 – 06/07
<input type="checkbox"/>	First ICD9 E-code (cause of injury)	85/86 – 06/07
<input type="checkbox"/>	First ICD10-CA E-code (cause of injury)	01/02 onward
<input type="checkbox"/>	Second ICD9 E-code (cause of injury)	85/86 – 00/01
<input type="checkbox"/>	ICD9 injury code (800-999)	85/86 – 06/07
<input type="checkbox"/>	ICD10-CA injury code (S00T98)	01/02 onward
<input type="checkbox"/>	Procedure code (CCP)	max. of 12 in 85/86 – 89/90; 10 in 90/91 – 00/01; and 20 in 01/02 – 06/07
<input type="checkbox"/>	Intervention code (CCI) (max. of 20 codes)	01/02 onward
<input type="checkbox"/>	Procedure on admission day indicator	
<input type="checkbox"/>	Procedure / intervention date	max. of 12 in 85/86 – 89/90; 10 in 90/91 – 00/01; and 20 in 01/02 onward
<input type="checkbox"/>	Procedure short list (based on CCP coding)	91/92 – 06/07
<input type="checkbox"/>	Intervention provider (procedure surgeon)	max. of 12 in 85/86 – 89/90; 10 in 90/91 – 00/01; and 20 in 01/02 onward
	Replaced by project-specific identification number	
<input type="checkbox"/>	Procedure surgeons' service	max. of 12 in 85/86 – 89/90; 10 in 90/91 – 00/01; and 20 in 01/02 onward
<input type="checkbox"/>	Intervention (procedure) anaesthetist	max. of 12 in 85/86 – 89/90; 10 in 90/91 – 00/01; and 20 in 01/02 onward
	Replaced by project-specific identification number	
<input type="checkbox"/>	Intervention (procedure) anaesthetic	max. of 12 in 85/86 – 89/90; 10 in 90/91 – 00/01; and 20 in 01/02 onward
<input type="checkbox"/>	Operative / non-operative	99/00 – 00/01
<input type="checkbox"/>	Operation group 1	90/91 – 06/07
<input type="checkbox"/>	Operation group 2	90/91 – 06/07
<input type="checkbox"/>	Operation group 3	90/91 – 06/07
<input type="checkbox"/>	Physiotherapy	85/86 – 00/01
<input type="checkbox"/>	Occupational therapy	85/86 – 00/01
<input type="checkbox"/>	Tertiary code 1	93/94 – 00/01
<input type="checkbox"/>	Tertiary code 2	93/94 – 00/01
<input type="checkbox"/>	Mother listed on newborn record	97/98 onward
	Replaced by project-specific identification number	
<input type="checkbox"/>	Gestational age	94/95 – 06/07
<input type="checkbox"/>	Clinical gestation weeks at admission	07/08
<input type="checkbox"/>	Clinical gestation weeks at delivery	07/08
<input type="checkbox"/>	Clinical gestation weeks at discharge	07/08
<input type="checkbox"/>	Infant birth weight	
<input type="checkbox"/>	Neonatal ICU level II days	93/94 – onward

<input type="checkbox"/>	Neonatal ICU level III days	93/94 – onward
<input type="checkbox"/>	Residence indicator	91/92 – 07/08
<input type="checkbox"/>	Province issuing health care number	91/92 – onward
<input type="checkbox"/>	Institution number for out of province facilities	91/92 – onward
<input type="checkbox"/>	Province code (location of hospital)	91/92 – onward
<input type="checkbox"/>	Responsibility for payment	
<input type="checkbox"/>	Third party liability form	
CIHI CMG with Complexity Grouper Variables/Day Procedure Groups		
<input type="checkbox"/>	CIHI case mix group (CMG)	91/92 – 00/01
<input type="checkbox"/>	CIHI major clinical category (MCC)	91/92 – 00/01
<input type="checkbox"/>	CIHI CMG age category	91/92 – 00/01
<input type="checkbox"/>	CIHI CMG complexity grade list indicator	91/92 – 00/01
<input type="checkbox"/>	CIHI CMG complexity/ co-morbidity level	91/92 – 00/01
<input type="checkbox"/>	CIHI expected length of stay (ELOS)	91/92 – 00/01
<input type="checkbox"/>	CIHI resource intensity weighting (RIW) value	91/92 – 00/01
<input type="checkbox"/>	CIHI resource intensity weighting (RIW) exclusion indicator / atypical code	91/92 – 00/01
<input type="checkbox"/>	CIHI day procedure group (DPG)	91/92 – 00/01
<input type="checkbox"/>	CIHI day procedure group (DPG) weight	91/92 – 00/01
CIHI CMG Plus Grouper Variables/Day Procedure Groups Plus		
<input type="checkbox"/>	Methodology version	01/02 – onward
<input type="checkbox"/>	Methodology year	01/02 – onward
<input type="checkbox"/>	MCC+	01/02 – onward
<input type="checkbox"/>	CMG+	01/02 – onward
<input type="checkbox"/>	CMG return code	01/02 – onward
<input type="checkbox"/>	MCC partition	01/02 – onward
<input type="checkbox"/>	Co-morbidity level	01/02 – onward
<input type="checkbox"/>	Co-morbidity total factor	01/02 – onward
<input type="checkbox"/>	CMG age category	01/02 – onward
<input type="checkbox"/>	Flagged intervention count	01/02 – onward
<input type="checkbox"/>	Intervention event count	01/02 – onward
<input type="checkbox"/>	Intervention OOH count	01/02 – onward
<input type="checkbox"/>	CMG intervention	01/02 – onward
<input type="checkbox"/>	CMG intervention status	01/02 – onward
<input type="checkbox"/>	CMG intervention location	01/02 – onward
<input type="checkbox"/>	CMG intervention extent	01/02 – onward
<input type="checkbox"/>	CMG intervention episode	01/02 – onward

<input type="checkbox"/>	Diagnosis used for CMG assignment	01/02 – onward
<input type="checkbox"/>	DPG+	01/02 – onward
<input type="checkbox"/>	DPG grouper return code	01/02 – onward
<input type="checkbox"/>	DPG RIW+	01/02 – onward
<input type="checkbox"/>	Inpatient RIW+	01/02 – onward
<input type="checkbox"/>	ELOS days	01/02 – onward
<input type="checkbox"/>	Inpatient RIW atypical code	01/02 – onward
<input type="checkbox"/>	Inpatient resource intensity level	01/02 – onward
<input type="checkbox"/>	Inpatient resource intensity total factor	01/02 – onward
<input type="checkbox"/>	Trim days	01/02 – onward
<input type="checkbox"/>	Cardioversion flag	01/02 – onward
<input type="checkbox"/>	Cell saver flag	01/02 – onward
<input type="checkbox"/>	Chemotherapy flag	01/02 – onward
<input type="checkbox"/>	Dialysis flag	01/02 – onward
<input type="checkbox"/>	Heart resuscitation flag	01/02 – onward
<input type="checkbox"/>	Mechanical ventilation ge 96 hours flag	01/02 – onward
<input type="checkbox"/>	Mechanical ventilation lt 96 hours flag	01/02 – onward
<input type="checkbox"/>	Feeding tube flag	01/02 – onward
<input type="checkbox"/>	Paracentesis flag	01/02 – onward
<input type="checkbox"/>	Parenteral nutrition flag	01/02 – onward
<input type="checkbox"/>	Pleurocentesis flag	01/02 – onward
<input type="checkbox"/>	Radiotherapy flag	01/02 – onward
<input type="checkbox"/>	Tracheostomy flag	01/02 – onward
<input type="checkbox"/>	Vascular access device flag	01/02 – onward

Project Title				Applies to Subpopulation(s)	
Date Range	yyyy/mm/dd	to	yyyy/mm/dd		
Other date range criteria:					

Home and Community Care file (previously Continuing Care) (January 1, 1990 onwards)	
All transactions relating to individuals receiving services paid for by the Home and Community Care Branch of the BC Ministry of Health Services; i.e., in-patients in HCC-funded institutions, clients in funded adult daycare programs, and clients receiving funded home care. Records include (1) client master records: demographic and related information; (2) assessment records; (3) advice for long term care (residential) records (advice as to what LTC care is approved for the client); and (4) advice for direct care service records (advice as to what external care is approved).	
CLIENT and CLIENT DEMOGRAPHIC FILES: Includes demographic and other information on the client.	
<input checked="" type="checkbox"/>	Client number Replaced by project-specific identification number (unless otherwise authorized) Note: Client numbers are provided to allow the grouping of service records within a single care episode.
<input type="checkbox"/>	Start date (from Client Demographic file)
<input type="checkbox"/>	End date (from Client Demographic file)
<input type="checkbox"/>	Status date
<input type="checkbox"/>	Referral status code
<input type="checkbox"/>	Responsible assessor ID Replaced by project-specific identification number
<input type="checkbox"/>	Direct care health unit (sub-office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Direct care health unit 2 (office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Home nursing care program (HNC) area code Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Home nursing care program (HNC) review date
<input type="checkbox"/>	Home service for community living (HSCL) care code
<input type="checkbox"/>	Long term care (LTC) health unit (sub-office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:

<input type="checkbox"/>	Long term care (LTC) health unit 2 (office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Long term care (LTC) review date
<input type="checkbox"/>	Review code
<input type="checkbox"/>	Need code
<input type="checkbox"/>	Marital code
<input type="checkbox"/>	Guaranteed annual income for need (GAIN) code
<input type="checkbox"/>	Guaranteed income supplement (GIS) code
<input type="checkbox"/>	Subsidy code
<input type="checkbox"/>	Subsidy effective date
<input type="checkbox"/>	War veteran allowance code
LONG TERM CARE ASSESSMENT FILE: Includes descriptions of all assessments for each long term care (LTC) client.	
<input checked="" type="checkbox"/>	Client number Replaced by project-specific identification number (unless otherwise authorized) Note: Client numbers are provided to allow the grouping of service records within a single care episode.
<input type="checkbox"/>	Assessment effective date
<input type="checkbox"/>	Most recent assessment code
<input type="checkbox"/>	Assessor ID Replaced by project-specific identification number
<input type="checkbox"/>	Location code
<input type="checkbox"/>	Assessment code
<input type="checkbox"/>	Approved care code
<input type="checkbox"/>	Approved care level code
<input type="checkbox"/>	Caregiver code
<input type="checkbox"/>	Assessment health unit (sub-office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Assessment health unit 2 (office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:

LONG TERM CARE SERVICE PLAN FILE: Includes the LTC service authorizations (SAs) for each client. Each record in the LTC Service Plan file is called a "service event." A service event is a period of service that a client has with a service provider. Each service event begins with a SA start or a SA change, and the event is either open or ended by a SA change or a SA end. Several service events are called a "service series." A service series that a client has with a provider begins with a SA start, may have one or more SA changes and may be either open or terminated by an SA end. Each LTC Service Plan record has the assessment effective date for the related assessment, found in the LTC Assessment file. The 'absolute start' and 'absolute end' fields refer to the dates and SA-IDs for the SA start and the SA end for a service series.

<input checked="" type="checkbox"/>	Client number Replaced by project-specific identification number (unless otherwise authorized) Note: Client numbers are provided to allow the grouping of service records within a single care episode.
<input type="checkbox"/>	Absolute start date
<input type="checkbox"/>	Absolute start service authorization (SA) ID Replaced by project-specific identification number
<input type="checkbox"/>	Absolute end date
<input type="checkbox"/>	Absolute end reason code
<input type="checkbox"/>	Absolute end service authorization (SA) ID Replaced by project-specific identification number
<input type="checkbox"/>	Start date
<input type="checkbox"/>	Start reason code
<input type="checkbox"/>	Start type code
<input type="checkbox"/>	Start service authorization (SA) ID Replaced by project-specific identification number
<input type="checkbox"/>	End date
<input type="checkbox"/>	End reason code
<input type="checkbox"/>	End type code
<input type="checkbox"/>	End service authorization (SA) ID Replaced by project-specific identification number
<input type="checkbox"/>	Assessment effective date
<input type="checkbox"/>	Care level code
<input type="checkbox"/>	Service event health unit (sub-office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Service event health unit 2 (office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Organizational code
<input type="checkbox"/>	Maximum authorized amount
<input type="checkbox"/>	CCD pays code

<input type="checkbox"/>	Client contribution amount
<input type="checkbox"/>	Provider category code
<input type="checkbox"/>	Service code
<input type="checkbox"/>	Service type code
<input type="checkbox"/>	Assessor ID Replaced by project-specific identification number
<input type="checkbox"/>	Provider ID Replaced by project-specific identification number
DIRECT CARE SERVICE PLAN FILE: Direct Care provides health care services to people in their homes. Services provided include nursing care and rehabilitation therapy (community physiotherapy and occupational therapy).	
<input checked="" type="checkbox"/>	Client number Replaced by project-specific identification number (unless otherwise authorized) Note: Client numbers are provided to allow the grouping of service records within a single care episode.
<input type="checkbox"/>	Start authorization date
<input type="checkbox"/>	Organization code
<input type="checkbox"/>	Service code
<input type="checkbox"/>	Service type code
<input type="checkbox"/>	DP health unit (sub-office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	DP health unit 2 (office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Treatment goal code
<input type="checkbox"/>	Care group type 1 code
<input type="checkbox"/>	Care group type 2 code
<input type="checkbox"/>	Care group type 3 code
<input type="checkbox"/>	Care level code
<input type="checkbox"/>	Expected program stay code
<input type="checkbox"/>	Referral source code
<input type="checkbox"/>	Hospital ID Replaced by project-specific identification number
<input type="checkbox"/>	Ward ID
<input type="checkbox"/>	Physician ID Replaced by project-specific identification number
<input type="checkbox"/>	Primary diagnostic code
<input type="checkbox"/>	Secondary diagnostic code

<input type="checkbox"/>	Operation surgery code
<input type="checkbox"/>	Provider ID Replaced by project-specific identification number
<input type="checkbox"/>	Occupational therapy (OT) or public health nurse (PHN) visits 1
<input type="checkbox"/>	OT or PHN visits 2
<input type="checkbox"/>	OT or PHN visits 3
<input type="checkbox"/>	OT or PHN visits 4
<input type="checkbox"/>	Physiotherapy (PT) or home nursing care (HNC) visits 1
<input type="checkbox"/>	PT or HNC visits 2
<input type="checkbox"/>	PT or HNC visits 3
<input type="checkbox"/>	PT or HNC visits 4
<input type="checkbox"/>	Visit last update date
<input type="checkbox"/>	Reason code
<input type="checkbox"/>	Patient outcome code
<input type="checkbox"/>	Authorization end date
GROUP HOME CLAIMS FILE: Group Homes are private residences ranging from single-family dwellings to apartment complexes that enable young adults with physical or mental disabilities to increase their independence by living in a community setting. Operated by non-profit or for profit societies, group homes usually accommodate four to six residents.	
<input checked="" type="checkbox"/>	Client number Replaced by project-specific identification number (unless otherwise authorized) Note: Client numbers are provided to allow the grouping of service records within a single care episode.
<input type="checkbox"/>	Care level code
<input type="checkbox"/>	Days of service amount
<input type="checkbox"/>	Hours of service amount
<input type="checkbox"/>	CK health unit (sub-office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	CK health unit 2 (office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Provider ID Replaced by project-specific identification number
<input type="checkbox"/>	Paid amount
<input type="checkbox"/>	Paid date
<input type="checkbox"/>	Rate amount
<input type="checkbox"/>	Rate code
<input type="checkbox"/>	Client contribution amount

<input type="checkbox"/>	Service authorization ID Replaced by project-specific identification number
<input type="checkbox"/>	Organization code
<input type="checkbox"/>	Service type code
<input type="checkbox"/>	Service month
<input type="checkbox"/>	Service year
ADULT DAY CARE CLAIMS FILE: Adult Day Care assists individuals to continue to live in their own homes by providing a variety of supportive programs in a group setting. The range of services and activities varies, but may include professional health care services, personal care services, therapeutic activities, and recreational and socialization activities. A nutritious noon meal and snacks are provided, and transportation to and from the centre to the client's residence is provided.	
<input checked="" type="checkbox"/>	Client number Replaced by project-specific identification number (unless otherwise authorized) Note: Client numbers are provided to allow the grouping of service records within a single care episode.
<input type="checkbox"/>	Care level code
<input type="checkbox"/>	Days of service amount
<input type="checkbox"/>	Hours of service amount
<input type="checkbox"/>	CJ health unit (sub-office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	CJ health unit 2 (office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Provider ID Replaced by project-specific identification number
<input type="checkbox"/>	Paid amount
<input type="checkbox"/>	Paid date
<input type="checkbox"/>	Rate amount
<input type="checkbox"/>	Rate code
<input type="checkbox"/>	Client contribution amount
<input type="checkbox"/>	Service authorization ID Replaced by project-specific identification number
<input type="checkbox"/>	Organization code
<input type="checkbox"/>	Service type code
<input type="checkbox"/>	Service month
<input type="checkbox"/>	Service year

HOME SUPPORT CLAIMS FILE: In-home support services provide a variety of supportive services to enable individuals with health related problems to remain in their own homes for as long as possible. Homemaker services provide personal assistance with daily activities, such as bathing, dressing and grooming. The homemaker can also assist with various household tasks including laundry, vacuuming and cooking.

<input checked="" type="checkbox"/>	Client number Replaced by project-specific identification number (unless otherwise authorized) Note: Client numbers are provided to allow the grouping of service records within a single care episode.
<input type="checkbox"/>	Care level code
<input type="checkbox"/>	Days of service amount
<input type="checkbox"/>	Hours of service amount
<input type="checkbox"/>	CI health unit (sub-office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	CI health unit 2 (office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Provider ID Replaced by project-specific identification number
<input type="checkbox"/>	Paid amount
<input type="checkbox"/>	Paid date
<input type="checkbox"/>	Rate amount
<input type="checkbox"/>	Rate code
<input type="checkbox"/>	Client contribution amount
<input type="checkbox"/>	Service authorization ID Replaced by project-specific identification number
<input type="checkbox"/>	Organization code
<input type="checkbox"/>	Service type code
<input type="checkbox"/>	Service month
<input type="checkbox"/>	Service year
DIRECT CARE DIAGNOSTIC: Includes diagnostic text descriptions for the Direct Care Service Authorizations. Note: There are no ICD9 codes in this table.	
<input checked="" type="checkbox"/>	Client number Replaced by project-specific identification number (unless otherwise authorized) Note: Client numbers are provided to allow the grouping of service records within a single care episode.
<input type="checkbox"/>	Effective date
<input type="checkbox"/>	Operation surgery diagnostic text
<input type="checkbox"/>	Primary diagnostic text
<input type="checkbox"/>	Secondary diagnostic text

<input type="checkbox"/>	Provider ID Replaced by project-specific identification number
PROVIDER and PROVIDER HISTORY FILES: Includes Provider demographics / information. Some provider information can change over time. The most current information is stored in the Provider file, and previous changes are stored in the Provider History file.	
<input type="checkbox"/>	Provider ID Replaced by project-specific identification number
<input type="checkbox"/>	Provider History from date
<input type="checkbox"/>	Provider History to date
<input type="checkbox"/>	Provider health unit (sub-office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Provider health unit 2 (office) ID Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Provider pay class code
<input type="checkbox"/>	Provider category code
<input type="checkbox"/>	Provider sub-category code
<input type="checkbox"/>	Provider is profit code
<input type="checkbox"/>	Responsible assessor ID Replaced by project-specific identification number
<input type="checkbox"/>	Provider status date
<input type="checkbox"/>	Provider active status code
<input type="checkbox"/>	Provider opening date

Project Title	Applies to Subpopulation(s)
----------------------	------------------------------------

Date Range	yyyy/mm/dd	to	yyyy/mm/dd
Other date range criteria:			

Mental Health Services File – Minimum Reporting Requirements (April 1, 1986 onwards)	
<p>Extract of the Minimum Reporting Requirement (MRR) tables from the Mental Health Data Warehouse. All health authorities in BC are required to report MRR data on all patient/clients receiving mental health services in the community.</p> <p>Note: Only Care Episodes and Service Events with a 'first contact date' greater than or equal to April 1, 1986 are included in the data.</p>	
CARE EPISODE FILE	
<input checked="" type="checkbox"/>	Care episode number Replaced by project-specific identification number (unless otherwise authorized) Note: Care episode number and project-specific Service event number are provided unless otherwise authorized. This allows the grouping of service records within a single care episode or service event.
<input type="checkbox"/>	Location code - Replaced by project-specific identification number OR Location code (unencrypted) – Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	First contact date
<input type="checkbox"/>	CPIM PharmaCare registration code
<input type="checkbox"/>	Residence at admission code
<input type="checkbox"/>	Referral source code
<input type="checkbox"/>	Referral date
<input type="checkbox"/>	DSM axis1 code 1
<input type="checkbox"/>	DSM axis1 code 2
<input type="checkbox"/>	DSM axis2 code 1
<input type="checkbox"/>	DSM axis4 code 1
<input type="checkbox"/>	DSM axis5 code 1
<input type="checkbox"/>	DSM axis5 code 2
<input type="checkbox"/>	Residence at discharge code
<input type="checkbox"/>	Referral target
<input type="checkbox"/>	Discontinue reason code
<input type="checkbox"/>	Discontinue date
<input type="checkbox"/>	Create date
SERVICE EVENTS FILE	

<input checked="" type="checkbox"/>	<p>Care episode number</p> <p>Replaced by project-specific identification number (unless otherwise authorized)</p> <p>Note: Care episode number and project-specific Service event number are provided unless otherwise authorized. This allows the grouping of service records within a single care episode or service event.</p>
<input checked="" type="checkbox"/>	<p>Service event number</p> <p>Replaced by project-specific identification number (unless otherwise authorized)</p> <p>Note: Care episode number and project-specific Service event number are provided unless otherwise authorized. This allows the grouping of service records within a single care episode or service event.</p>
<input type="checkbox"/>	<p>Location code - Replaced by project-specific identification number</p> <p><u>OR</u></p> <p><input type="checkbox"/> Location code (unencrypted) – Research rationale describing why this field is required must be supplied before it will be considered for release:</p>
<input type="checkbox"/>	First contact date
<input type="checkbox"/>	Service event code
<input type="checkbox"/>	Service event date
<input type="checkbox"/>	Employment status code
<input type="checkbox"/>	Vocational status code
<input type="checkbox"/>	Marital status code
<input type="checkbox"/>	Household composition code
<input type="checkbox"/>	Education level code
<input type="checkbox"/>	Create date

Project Title	Applies to Subpopulation(s)
----------------------	------------------------------------

Date Range	yyyy/mm/dd	to	yyyy/mm/dd
Other date range criteria:			

Medical Services Plan payment information file (April 1, 1985 onwards)	
Fiscal year files of services provided to MSP-covered individuals by fee-for-service practitioners, billed to MSP, and paid by MSP. Practitioners billing MSP are separated into three groups: physicians, supplementary benefit practitioners (physiotherapists, massage practitioners, naturopathic physicians, etc.), and out-of-province practitioners, including claims paid for by third parties such as ICBC and WorkSafeBC. These data do NOT include therapeutic abortion data in accordance with the BC Freedom of Information and Protection of Privacy Act.	
<input type="checkbox"/>	Service date
<input type="checkbox"/>	Paid for item (fee item)
<input type="checkbox"/>	Service code
<input type="checkbox"/>	ICD9 diagnostic code (first included in 91/92)
<input type="checkbox"/>	Paid service units
<input type="checkbox"/>	Paid amount
<input type="checkbox"/>	Explanatory code
<input type="checkbox"/>	Date paid
<input type="checkbox"/>	Payment receiver code
<input type="checkbox"/>	Payee number Replaced by project-specific identification number
<input type="checkbox"/>	Subsidy code
<input type="checkbox"/>	Claim type (first included in 99/00)
<input type="checkbox"/>	Practitioner number Replaced by project-specific identification number
<input type="checkbox"/>	Claim specialty code
<input type="checkbox"/>	Referring practitioner number Replaced by project-specific identification number
<input type="checkbox"/>	Client Province (first included in 88/89)
<input type="checkbox"/>	Service where code
<input type="checkbox"/>	Location of the service (first included in 94/95)
Several additional fields detail retroactive and rollback payments are available from 1994/95 onwards. These are usually only necessary for projects involving these specific topics. Please contact Population Data BC for more information.	

Project Title	Applies to Subpopulation(s)
----------------------	------------------------------------

Date Range	yyyy/mm/dd	to	yyyy/mm/dd
Other date range criteria:			

PharmaCare file (January 1, 1985 onwards)	
<p>Prescriptions paid for through the BC PharmaCare program. Please note, with the introduction of the income-based Fair PharmaCare plan on May 1, 2003, the plan benefit structure changed and thus the data available before and after this date will not be readily comparable. Visit the Population Data BC web site (http://www.popdata.bc.ca) and the Ministry of Health Services PharmaCare web site (http://www.health.gov.bc.ca/pharme/index.html) for further details on the program and plan types.</p>	
<p>Plan types available prior to May 1, 2003 (please choose one or more of the following):</p> <p> <input type="checkbox"/> Plan type A <input type="checkbox"/> Plan type B <input type="checkbox"/> Plan type C <input type="checkbox"/> Plan type D <input type="checkbox"/> Plan type E <input type="checkbox"/> Plan type F <input type="checkbox"/> Plan type G <input type="checkbox"/> All Plan types (A-G) </p> <p>Only records that have the selected plan type code(s) will be released.</p>	
<p>Plan types available after the introduction of Fair PharmaCare on May 1, 2003 (please choose one or more of the following):</p> <p> <input type="checkbox"/> Fair PharmaCare <input type="checkbox"/> Plan type B <input type="checkbox"/> Plan type C <input type="checkbox"/> Plan type D <input type="checkbox"/> Plan type F <input type="checkbox"/> Plan type G <input type="checkbox"/> Palliative Care Benefits Plan (Plan type P) <input type="checkbox"/> BC Centre for Excellence in HIV/AIDS <input type="checkbox"/> All Plan types </p> <p>Only records that have the selected plan type code(s) will be released.</p>	
<input type="checkbox"/>	Date of service (date prescription dispensed)
<input type="checkbox"/>	Drug number/ Canadian drug identity code (CDIC)
<input type="checkbox"/>	Therapeutic class code (must be requested with Drug Number/CDIC code above)
<input type="checkbox"/>	Days' supply accepted
<input type="checkbox"/>	Days' supply dispensed
<input type="checkbox"/>	Quantity accepted
<input type="checkbox"/>	Quantity dispensed
<input type="checkbox"/>	Ingredient cost accepted
<input type="checkbox"/>	Ingredient cost claimed
<input type="checkbox"/>	Ingredient cost paid
<input type="checkbox"/>	Professional fee accepted
<input type="checkbox"/>	Professional fee claimed
<input type="checkbox"/>	Professional fee paid
<input type="checkbox"/>	Product selection 1996 - 1999
<input type="checkbox"/>	Special authority
<input type="checkbox"/>	Special authority low cost alternative
<input type="checkbox"/>	Special authority non benefit

<input type="checkbox"/>	Special authority reference drug program	
<input type="checkbox"/>	Subsidy indicator	1994 - 1999
<input type="checkbox"/>	Accumulated expenditure amount (first included in 2000)	
<input type="checkbox"/>	Total copayment (first included in 2000)	
<input type="checkbox"/>	Total amount paid	
<input type="checkbox"/>	Practitioner number Replaced by project-specific identification number	

Project Title	Applies to Subpopulation(s)
----------------------	------------------------------------

Date Range	yyyy/mm/dd	to	yyyy/mm/dd
Other date range criteria:			

PharmaNet Files (January 1, 1996 to present)

PharmaNet data includes records of all medications dispensed in community pharmacies in BC. PharmaNet dispense data is available from two files; medication history and claims history. Medication history contains records for all dispenses in BC regardless who pays for the claim. Claims history contains claim records for all dispenses except those for individuals who are known to be federally insured (Veterans, RCMP, Armed Forces and beneficiaries of Non-Insured Health Benefits).

PharmaNet does **not** capture:

- Medications administered to hospital in-patients
- Antiretroviral medications dispensed from the Centre of Excellence in HIV / Aids at St. Paul's Hospital
- Chemotherapy agents dispensed by the BC Cancer Agency
- Medications purchased without a prescription may not be on PharmaNet (e.g., over the counter medications, herbal products, vitamins)
- Medication samples dispensed at a physician's office (some are entered by physicians with PharmaNet access)
- Third party paid amounts
- Medication cost information for federally insured individuals (RCMP, Canadian Forces, Veterans and beneficiaries of Non-Insured Health Benefits Program)

PATIENT INFORMATION

☐ PHN
Replaced by project-specific patient identification number

☐ Gender

☐ Date of birth (YYYYMM)

☐ Age (*calculated as of Jan 1 for each year of data*)

☐ Patient Health Authority (HA)

☐ Patient Local Health Area (LHA) – **Research rationale describing why this field is required must be supplied before it will be considered for release:**

☐ Other patient geographic information (Please Describe:) – **Research rationale describing why this field is required must be supplied before it will be considered for release:**

PHARMACY INFORMATION

☐ Pharmacy identification number
Replaced by project-specific pharmacy identification number

☐ Pharmacy Health Authority (HA)

☐ Pharmacy Local Health Area (LHA) – **Research rationale describing why this field is required must be supplied before it will be considered for release:**

<input type="checkbox"/>	Other pharmacy geographic information (Please Describe:) – Research rationale describing why this field is required must be supplied before it will be considered for release:
PRACTITIONER INFORMATION	
<input type="checkbox"/>	Practitioner identification number Replaced by project-specific practitioner identification number
<input type="checkbox"/>	Practitioner Health Authority (HA)
<input type="checkbox"/>	Practitioner Local Health Area (LHA) – Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Other Practitioner geographic information (Please Describe:) – Research rationale describing why this field is required must be supplied before it will be considered for release:
<input type="checkbox"/>	Practitioner identification reference (<i>code identifying the governing body from which practitioner receives licence</i>)
<input type="checkbox"/>	Practitioner type (<i>e.g., physician, dentist, nurse practitioner, podiatrist, midwife, veterinarian, pharmacist</i>)
<input type="checkbox"/>	Practitioner specialty flag Y/N
<input type="checkbox"/>	Practitioner specialty type description (<i>e.g., cardiology, neurology, paediatrics, urology</i>)
RECORDS REQUESTED FOR (Choose one of the following):	
<input type="checkbox"/>	All medications
<input type="checkbox"/>	Medications for drugs listed in drug file provided by applicant
<input type="checkbox"/>	Multiple drug lists provided. Please describe drug list use by cohort (i.e. use drug list 1 for cohort 1):
DRUG INFORMATION	
<input type="checkbox"/>	DINPIN (<i>drug information number as per drug list provided, field is mandatory</i>)
<input type="checkbox"/>	Canadian brand name
<input type="checkbox"/>	Chemical/generic name
<input type="checkbox"/>	GCN sequence number (<i>random number representing generic formulation of drug assigned by Health Canada</i>)
<input type="checkbox"/>	Drug strength
<input type="checkbox"/>	Drug form units (<i>e.g., ml, grams, each</i>)
<input type="checkbox"/>	Dosage form code and description (<i>e.g., aerosol, tablet, capsule, liquid</i>)
<input type="checkbox"/>	AHFS code (<i>American Hospital Formulary code assigned and maintained by Health Canada</i>)
<input type="checkbox"/>	PharmaCare Theraclass (<i>PharmaCare therapeutic class assigned and maintained by PharmaCare</i>)
MEDICATION REVIEW	
<input type="checkbox"/>	Medication Review Records (<i>as of April 1, 2011</i>) NOTE: <i>claims record field values: PIN = 99000501 or 99000502 or 99000503, drug cost = 0, quantity and days supply = 1 and prescriber type = pharmacist. (Standard 99000501, Pharmacist</i>

MEDICATION/DISPENSING INFORMATION

- ☐ Date of service (*date dispensed*)
- ☐ Quantity dispensed
- ☐ Days supply (*estimate of number of days of prescription treatment*)
- ☐ Directions for use (*80 character free format text field*)

CLAIMS INFORMATION

- ☐ Date of service (*date dispensed*)
- ☐ Account code and description (*Account type under which claim adjudicated*)
- ☐ Quantity (*actual quantity dispensed*)
- ☐ Quantity accepted (*pro-rated based on days supply accepted for payment by PharmaCare*)
- ☐ Days supply (*estimate number of days of treatment as submitted by pharmacist*)
- ☐ Days supply accepted (*submitted amount may be reduced if greater than Special Authority, plan or DINPIN amount*)
- ☐ Drug cost claimed by pharmacist
- ☐ Drug cost accepted by pharmacist
- ☐ Drug cost paid (*submitted drug cost amount paid by PharmaCare*)
- ☐ Professional fee (*dispensing fee claimed by pharmacist*)
- ☐ Professional fee accepted (*dispensing fee amount accepted by PharmaCare*)
- ☐ Professional fee paid (*dispensing fee amount paid by PharmaCare*)
- ☐ Special services fee (*total amount claimed by pharmacist for special service e.g., consulted prescriber, action Rx issue*)
- ☐ Special services fee paid (*PharmaCare paid amount to pharmacy for special service*)
- ☐ Copay to collect (*patient paid amount per claim*)
NOTE: to determine annual out of pocket expenses by PHN, total copay to collect amount for each PHN by year.
- ☐ Total amount paid (*PharmaCare amount paid for drug cost and professional fee*)
- ☐ Special authority flag Y/N
- ☐ Special authority type (*e.g., non-benefit, low cost alternative (LCA) or reference drug program; RDP*)
- ☐ Accumulated expenditure amount (*first included in 2000*)
- ☐ Claim Status
- ☐ Intervention Type Code

Additional Information/Comments:

Data Access Request (DAR)**Continuous Improvement – Deliverables**

	Enhancements	Action
1.	DARTS database – update, streamline & standardize	COMPLETE– April 2013
2.	Prepublication Review Submission process - streamline & standardize	COMPLETE – July 2013
3.	Project Closure process - streamline & standardize	COMPLETE – April 2013
4.	Academic Health Data Requests process - streamline & standardize	COMPLETE – April 2013
5.	Health Data Central Website – develop and implement	COMPLETE – May 2013
6.		
7.		

Monthly Ethics Report

July 2013 expiries:

Project Name	Project Number	Ethics Certificate Number	Ethics Expiry Date	Results
Tyndall	04-011	H02-50263	22-Jul-2013	Ethics renewal to June 18, 2014
Dahlgren	04-018	H03-70343	8-Jul-2013	Ethics renewal to June 10, 2014
Davies-KoeHoorn	05-003	H04-80270	30-Jul-2013	Ethics renewal to July 16, 2014
McBride	05-036	H05-60113	10-Jul-2013	Ethics renewal to June 26, 2014
McBride	09-015	H09-01957	10-Jul-2013	Ethics renewal to July 9, 2014
Khan	09-016	H08-02579	8-Jul-2013	Ethics renewal to June 26, 2014
Wong	10-014	H10-01417	5-Jul-2013	Email sent to MOH indicating closure in process July 4, 2013.
McGrail	10-015	H10-02693	5-Jul-2013	Ethics renewal to May 17, 2014
Wong	11-001	H10-02355	18-Jul-2013	Ethics renewal to June 26, 2014
Palepu	11-014	U of Ottawa 04-08-09	9-Jul-2013	Outstanding (MOH notified July 8, 2013)
Dahlgren	12-009	CW10-0176/ H10-00336	17-Jul-2013	Ethics renewal to July 8, 2014

Outstanding from previous months:

Project Name	Project Number	Ethics Certificate Number	Ethics Expiry Date	Status
Stothers	11-006	H03-70638	9-Nov-2012	Res. has not yet received data; data will not be released without ethics renewal.

Academic Research - Data Access Request (DAR) Process – Detailed

1. Completing the Data Access Request

The researcher works with Population Data BC staff in completing the data access request and preparing the application package.

The researcher works with Research Liason Unit (RLU) staff at Population Data BC in completing the data access request (DAR) and preparing the application package.

Current RLU Staff

Kelly Alke – 604-822-5206

Tim Choi – 604-822-5258

Monique Gagne – 604-822-3039

Sherylyn Arabsky – 604-822-1732

Maryam Matean – 604-822-6174

2. Submission to the Ministry

Population Data BC, on behalf of the researcher, submits the application package to the ministry for review.

The RLU emails the DAR and application package to the Data Access Research & Stewardship (DARS) unit at Ministry of Health.

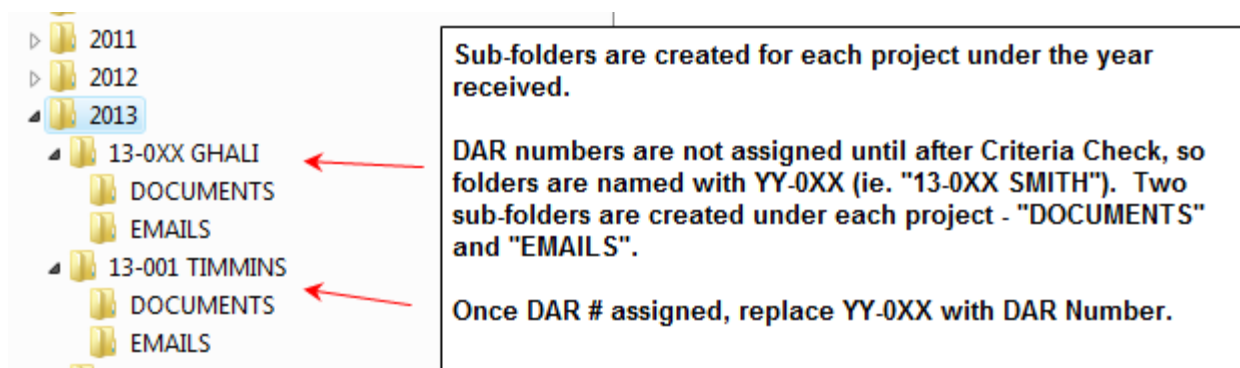
The Administrator (currently Shara Orr) forwards the new DAR package to the appropriate Analyst.

- Cornel Lencar if the DAR has a PharmaNet (PNet) or Request to Contact (RTC) component
- Rosemary Armour if there is no PNet component

The Administrator creates a folder for the DAR project and saves the email and supporting documentation to the LAN

s. 15

See below folder structure creation format:



Administrator saves the original email in the EMAIL folder and each supporting document in the DOCUMENTS folder. All emails and documentation are to be saved with the following format:

YYYY-MM-DD – 'meaningful description of email/doc' – RESEARCHER_LASTNAME – DAR# (when available)

See examples below:

EMAILS

- ✉ 2013-06-20 - PopData sends New DAR and supporting docs - Hedden.msg
- ✉ 2013-07-03 - Cornel sends Shara his prelim review of DAR - 13-0XX HEDDEN.msg
- ✉ 2013-07-04 - MoH sends Criteria Check email with Category and DAR number - 13-033 - Hedden.msg

DOCUMENTS

- 📄 2013-06-20 - DAR - Hedden.pdf
- 📄 2013-06-20 - DAR Checklist_Consolidation File - Hedden.doc
- 📄 2013-06-20 - DAR Checklist_DAD - Hedden.doc
- 📄 2013-06-20 - DAR Checklist_MSP - Hedden.doc
- 📄 2013-06-20 - DAR Checklist_VS Deaths - Hedden.doc
- 📄 2013-06-20 - DAR Cover Letter - Hedden.docx
- 📄 2013-06-20 - DAR Signature Page - Hedden.pdf
- 📄 2013-06-20 - Ethics Application - Hedden.pdf
- 📄 2013-06-20 - Ethics Approval - Hedden.pdf
- 📄 2013-06-20 - Letter from committee - Hedden.pdf
- 📄 2013-06-20 - List of External Data Fields_Applies Cohort 1(Physicians) - Hedden.docx
- 📄 2013-06-20 - MoH Application Summary - Hedden.docx
- 📄 2013-06-20 - Request for CPSBC data - Hedden.docx

Administrator records New/Pending DARS on Criteria Check Queue Whiteboard:

** Criteria Check Queue Whiteboard is located across from Karen Li's cubicle (between Pillar C0 and C1)
**

Researcher Name	Date Recd	Analyst Assigned	Criteria Check due date
Brubacher	Aug 8 (off hold)	Cornel	Aug 22
Ghali	Aug 13 (re-submission with ethics waiver)	Rosemary	Aug 27

- Researchers Name
- Date Request Received
- Analyst Assigned
- Date Criteria Check Due (2 weeks from received Date)

3. Criteria Check

The ministry performs a criteria check within two weeks of receiving a new application package. The criteria check is a preliminary assessment of any major issues, including completeness and accuracy. The ministry will then assign a project number and a corresponding category. Details regarding project categories are provided at the following website:

<http://www.popdata.bc.ca/news/NewMoHApprovalProcess>

If the application package does not meet the requirements of the criteria check, it will be returned to Population Data BC to work with the researcher for revision and resubmission.

The Administrator forwards a list of team members on the project (indicating those who require access to data) to **Audit Team** (currently Carlos Caraveo Carlos.Caraveo@gov.bc.ca - A/Director, Knowledge Integration and Development, Health Sector IM/IT) for review. Carlos will review the list of team members for issues/conflicts and will advise if there are any issues and whether or not the request can proceed. This review can be happening concurrently with the Criteria Check.

The Analyst conducts the Criteria Check on the DAR application. The Criteria Check must be completed **within 2 weeks** of receipt of the DAR application.

The Analyst reviews on the following:

Completeness and Consistency:

- Check that Project Title, Team Members and Roles, and all project details are consistent between all documentation – DAR, Ethics Application, Funding, etc.
- If there is a difference in Project Titles between documentation, ensure justification is provided
- Check that the data dates requested in the DAR are consistent with those in the Checklists
- Check that the Cohort definitions and dates requested on the Checklists are consistent with the DAR
- Check if a Peer Review has been conducted (ie through a funding agency). If not, ensure a Project Proposal is provided

Appropriateness:

- Check that the methodology is clear, while providing an appropriate level of detail
- Check that sound rationale is provided for each database being requested
- Evaluate methodology and the data requested, while respecting the 'Need to Know' principle
- Review Checklists for sensitive data variables being request. If so, ensure strong rationale is provided
- Review accuracy of the Linkage Strategy
- If funded by private industry, ensure the following criteria is met:
 - (a) the research is conducted at arm's length from the sponsor;
 - (b) no sponsor's employees, contractors, or agents are part of the project team;
 - (c) the sponsor has no influence on study direction or analysis; and
 - (d) the sponsor has no access to data, other than final published results.
-

Often through the Criteria Check process, questions arise or clarifications are required. **The Analyst** will make note of these and bring them to the DARS weekly Team Round Table Meeting (**Round Table**).

The Analyst determines the Process Category based on the information in the DAR and the guidelines published on the PopData website: <http://www.popdata.bc.ca/news/NewMoHApprovalProcess>

The Analyst briefs the team on the file and all initial questions during **Round Table**. Other members of the team have an opportunity to ask questions about the project. If these questions are deemed valid and appropriate, **The Analyst** adds them to the list of questions for the researcher.


If the Project passes the criteria check and is being accepted for review, **The Analyst** then enters the project into the DARTS database as following:

DARTS - Data Access Request Tracking System

<input type="checkbox"/> Data Entry Form	<input type="checkbox"/> Performance Measurement Report
<input type="checkbox"/> DAR Summary Report	<input type="checkbox"/> Add/Edit Researchers
<input type="checkbox"/> Data File/Source Report	<input type="checkbox"/> Add/Edit Steward List
<input type="checkbox"/> DAR Status Report	<input type="checkbox"/> Add/Edit Database List
<input type="checkbox"/> DARS Audit Report	<input type="checkbox"/> Add/Edit Status
<input type="checkbox"/> Proposal History Report	<input type="checkbox"/> Add/Edit Dropdown Lists
<input type="checkbox"/> Research Web Export	<input type="checkbox"/> Add/Edit Process Category
<input type="checkbox"/> Amendments Status Report	<input type="checkbox"/> Add/Edit Attachment/Doc Type
<input type="checkbox"/> DARS Status Report	<input type="checkbox"/> Add/Edit Publication Type
<input type="checkbox"/> Search	<input type="checkbox"/> Check PrePub Review Due

Click 'Data Entry Form' to create/view Projects

V. 3.8 April 16, 2013

+

Notes

DARTS - Data Entry

Go to Request:
New
Name: Saadatsafavi, Mohsen
Select type of request/project (ok to select more than 1)
Close

Request No.: **13-035**

Title: *Continuity, Regularity, and Speciality in COPD Care: An Exploration of Long-term Costs and Health Outcomes*

ISA: ☐ HA: ☐ DAR: ☒ PNET: ☐

DAS: ☐ RTC: ☐ MOU: ☐ Other: ☐

Date Initiated: 04-Jul-13

Popdata No.:

PNet/CeRTS No.:

Click 'New' to create a new record/project

Click in Title box to enter Title

Project Team

Project Details

Security

Cohorts

Project Cycle Notes

Status History

Amendment

Post Agreement

Attachment

Principal Investigator/Requestor: Saadatsafavi, Mohsen Access: ☒ Pledge Signed: ☐

Co-Investigators

Co-Investigators	Access	Pledge Signed	
Lynd, Larry	<input checked="" type="checkbox"/>	<input type="checkbox"/>	?
FitzGerald, Mark	<input type="checkbox"/>	<input type="checkbox"/>	?
Marra, Carlo	<input checked="" type="checkbox"/>	<input type="checkbox"/>	?
Stirling, Bryan	<input type="checkbox"/>	<input type="checkbox"/>	?
Sin, Don	<input type="checkbox"/>	<input type="checkbox"/>	?
McGrail, Kim	<input type="checkbox"/>	<input type="checkbox"/>	?
*	<input type="checkbox"/>	<input type="checkbox"/>	?

Indicate if individual requires access to data

Team Members

Team Members	Access	Pledge Signed	
Galo, Jessica	<input type="checkbox"/>	<input type="checkbox"/>	?
Grubisic, Maja	<input checked="" type="checkbox"/>	<input type="checkbox"/>	?
Zafar, Zafar	<input checked="" type="checkbox"/>	<input type="checkbox"/>	?
Raymakers, Adam	<input checked="" type="checkbox"/>	<input type="checkbox"/>	?
Chen, Wenji	<input type="checkbox"/>	<input type="checkbox"/>	?
*	<input type="checkbox"/>	<input type="checkbox"/>	?

Use dropdown menu to select from existing individuals. If not in list Double Click on Principal Investigator box to enter new member

DARTS - Data Entry

Go to Request:
New
Name: Saadatsafavi, Mohsen
Current Status: Questions to PopData
Close

Request No.: **13-035**

Title: *Continuity, Regularity, and Speciality in COPD Care: An Exploration of Long-term Costs and Health Outcomes*

ISA: ☐ HA: ☐ DAR: ☒ PNET: ☐

DAS: ☐ RTC: ☐ MOU: ☐ Other: ☐

Date Initiated: 04-Jul-13

Popdata No.:

PNet/CeRTS No.:

Project Team

Project Details

Security

Cohorts

Project Cycle Notes

Status History

Amendment

Post Agreement

Attachment

Peer Review: Funding Source: N/A Ethics Review: Copv Attached Process Category: D

CV Attached ☐ Funding Expiry Date: Version #: H13-00684 3 mth Start Date:

Linkage - Y/N: ☐ Ethics Expiry Date: 03-Apr-14 End Date:

Resource Allocation: Cornel Lencar PIA Required: ☐ PIA Completed: ☐ STRA: ☐

Data Steward Approvals

Please select a database for review: 6 Databases have been selected.

Database / Steward	Date Range	Date Sent	Status	
Continuing Care / Deb McGinnis	1996/01/01-2012/12/31	24-Jun-13	Pending	09-Jul-13
Hospital Separations (DAD) / Deb McGinnis	1996/01/01-2012/12/31	24-Jun-13	Pending	09-Jul-13
MSP Payment Information Master / Deb McGinnis	1996/01/01-2012/12/31	24-Jun-13	Pending	09-Jul-13
MSP Registration and Premium Billing (RP&B) / Deb McGinnis	1996/01/01-2012/12/31	24-Jun-13	Pending	09-Jul-13
PharmaNet / Bruce Carleton	1996/01/01-2012/12/31	24-Jun-13	Pending	09-Jul-13
Vital Statistics Deaths / Jack Shewchuk	1996/01/01-2012/12/31	24-Jun-13	Pending	09-Jul-13

Select db requested from dropdown menu and input Data Ranges requested and status of request

DARTS - Data Entry Close

Go to Request: New

Request No.: **13-035**

Title: *Continuity, Regularity, and Specialty in COPD Care: An Exploration of Long-term Costs and Health Outcomes*

Name: **Saadatsafavi, Mohsen**

Current Status: **Questions to PopData**

Date Initiated: 04-Jul-13

Popdata No.:

PNet/CeRTS No.:

ISA: ☐ HA: ☐ DAR: ☒ PNET: ☐

DAS: ☐ RTC: ☐ MOU: ☐ Other: ☐

Project Team | Project Details | **Security** | Cohorts | Project Cycle Notes | Status History | Amendment | Post Agreement | Attachment

Individuals to be Contacted: No

Format of Birth/Death Date: Y/M Only

Linkages to Other Data: No

Personally Identifiable Info:

Data Transfer:

GeoCode: SES

HA

HSDA

LHA

CD

Data Storage/Access

Office: ☐ PC: ☐

SRE: ☐ Server/MF: ☐

Location of Notes, Etc.:

Personally Identifiable Info Details/Comments:

DARTS - Data Entry Close

Go to Request: New

Request No.: **13-035**

Title: *Continuity, Regularity, and Specialty in COPD Care: An Exploration of Long-term Costs and Health Outcomes*

Name: **Saadatsafavi, Mohsen**

Current Status: **Questions to PopData**

Date Initiated: 04-Jul-13

Popdata No.:

PNet/CeRTS No.:

ISA: ☐ HA: ☐ DAR: ☒ PNET: ☐

DAS: ☐ RTC: ☐ MOU: ☐ Other: ☐

Project Team | Project Details | Security | **Cohorts** | Project Cycle Notes | Status History | Amendment | Post Agreement | Attachment

Cohort Type	Cohort Description	Defined By
▶ Cohort 1	All those meeting COPD def (see DAR) between 1/1/96-12/31/12	DAD & MSP
Control 1	2 matched controls for every 1 in cohort -match on Yr of birth, Sex, HSDA an	
*		

Record: 1 of 2

No Filter Search

DARTS - Data Entry

Go to Request:

Request No.: **13-035**

Title: *Continuity, Regularity, and Specialty in COPD Care: An Exploration of Long-term Costs and Health Outcomes*

Name: **Saadatsafavi, Mohsen**

ISA: ☐ HA: ☐ DAR: ☒ PNET: ☐

DAS: ☐ RTC: ☐ MOU: ☐ Other: ☐

Current Status: **Questions to PopData**

Date Initiated: **04-Jul-13**

Popdata No.:

PNet/CeRTS No.:

Project Team | Project Details | Security | Cohorts | Project Cycle Notes | **Status History** | Amendment | Post Agreement | Attachment

New Status: Date:

Comments:

Date	Status	Status Comments
04-Jul-13	Questions to PopData	
04-Jul-13	Request Acknowledged	Request Acknowledged = 'Criteria Check' email sent
24-Jun-13	Request Received	

The Analyst emails the Criteria Check confirmation to the RLU (rlu@popdata.bc.ca). This email is to include the new DAR # (obtained through the DARTS database), Process Category and time commitment (if applicable) and all questions/clarification that arose through the Criteria Check.

See below for a sample template:

Good Morning/Afternoon

Thank you for submitting the Data Access Request and supporting documentation on behalf of XXX for the project titled, "XXX", received by the Ministry of Health on XXX.

This project reference number is **XX-XXX** and this is a Category **X**.

[We do not have any preliminary questions at this time.]

[Please find below a list of our preliminary questions:]

Inconsistencies:

Clarification Questions:

Thank you,

IMPORTANT:

*The Analyst must ensure they 'cc' the DARS Inbox (HealthDataResearch@gov.bc.ca) on **ALL** correspondence, as the Administrator will save all emails in the appropriate LAN location and update the DARTS database accordingly*

The Analyst erases the corresponding project from the Criteria Check Queue whiteboard.

4. In-depth Review

Once an application package has passed the criteria check, it is reviewed by a ministry analyst for appropriate use of the data according to legislation and policy. Part of the review process may include follow-up clarification questions to the researcher.

When the in-depth review is complete, the application package and recommendation is submitted to the chief data steward for decision.

*The Analyst reviews responses from researcher to the initial questions sent out from Criteria Check. If further questions or clarifications are required, the Analyst will ask the RLU to schedule a teleconference (T/C) with MoH, the researcher and the RLU. The Analyst ensures that all issues are discussed to his/her satisfaction during the T/C. The RLU is responsible for capturing minutes/discussion from the T/C (usually in the form of a Clarifications Doc) and disseminate to stakeholders. **This is intended to be the only round of clarifications/communications.***

*When the Analyst determines that the in-depth review is complete and ready for decision, he/she prepares the Project Summary and takes the file to **Round Table** to review responses from questions and T/C discussion. Team Members ensure questions/concerns have been addressed satisfactorily. Project Summary template is located at [DARS Project Summary](#). Project Summary should not be more than 2 pages.*

5. Data Steward Decision and Notification

The chief data steward reviews the application package and approves or rejects the application.

The ministry sends a decision letter to the researcher, with copies to Population Data BC and all relevant data stewards.

If submitting for approval, the Analyst prepares Approval Letter for signature by the Chief Data Steward (CDS). Approval Letter template is located at [MOH Approval Letter](#). Please ensure the researcher's address and ethics expiry date are accurate, all involved Data Stewards are copied, and date is the following Monday.

Once Approval Letter has been created, the Analyst create a new folder under the "Approvals for Signature" folder s. 15 ith the Project # and Researchers Name as the folder title.

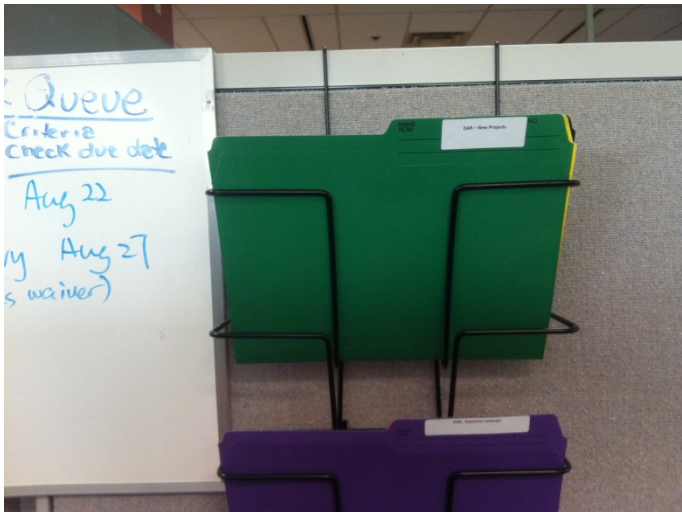
Save a copy of the Approval Letter in this folder, along with the:

- *Project Summary*
- *DAR*
- *copies of all Checklists*

- Clarifications/Modifications Doc(s) from PopData

The Analyst is to put paper copies of the Project Summary and Approval Letter in the 'DAR Approvals' Folder (green) and notify Karen.

*** Approval Folder (Green) is located across from Karen Li's cubicle (between Pillar C0 and C1), next to whiteboard ***



Karen will coordinate signing with CDS and setup time for briefing if project is complex or sensitive in nature.

Once the Approval Letter has been signed by the CDS, Karen will hand off to **the Administrator**.

The Administrator will:

- Scan a copy (pdf) of the Signed Approval Letter and save it to project folder
- Mail the signed hard copy to the researcher
- Email a copy of the Signed Approval Letter to RLU
- Update the DARTS db – Status, Data Retention Date
- Save Approval Letter and Project Summary from "Approvals for Signature" folder to the Project folder (replacing the existing copy)
- Delete all other files from the "Approvals for Signature" (project specific) folder
- Amend Project Updates document to reflect MoH Approval
- Update tracking spreadsheet - [PopData Academic Requests Tracking Document](#)

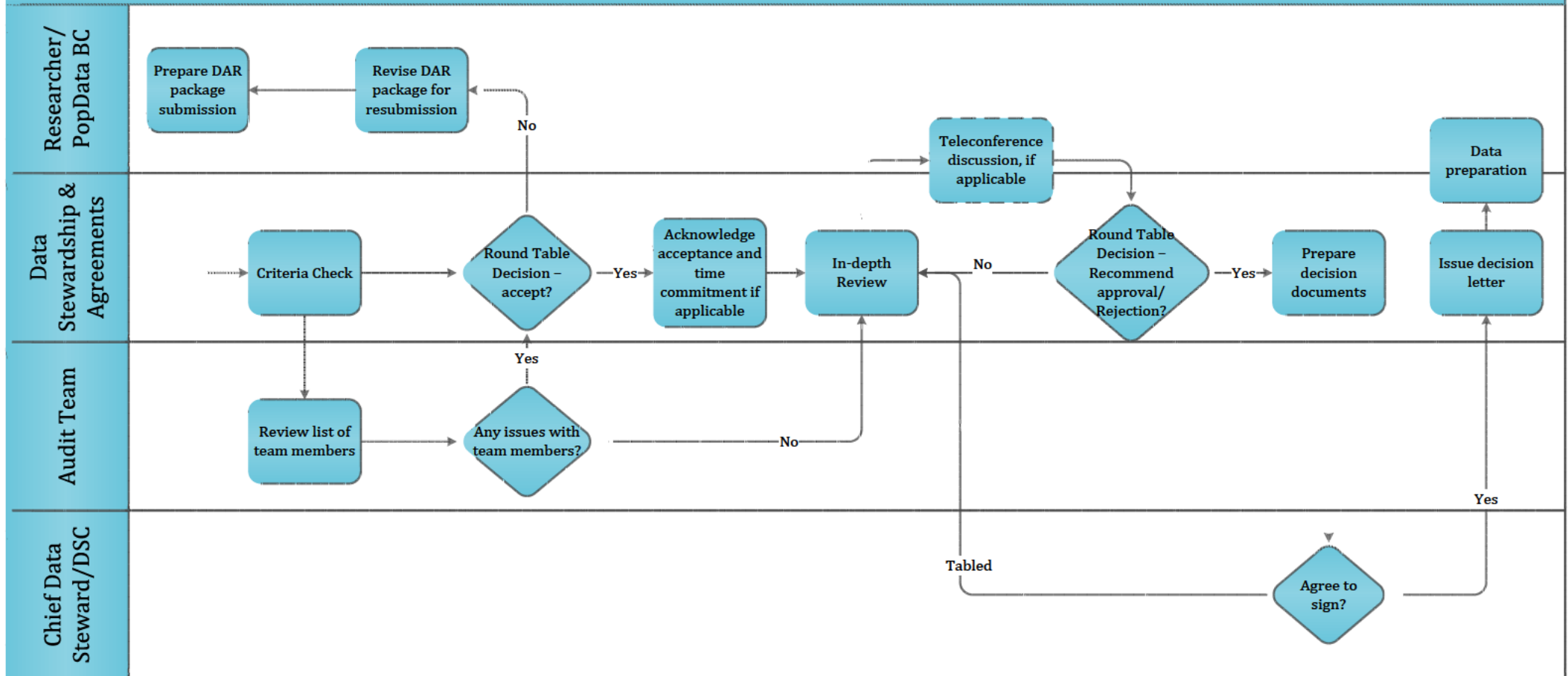
6. Data Preparation and Delivery

If the application is approved by all relevant data stewards, Population Data BC begins data preparation activities.

From here, data will be released to the researcher according to the specifications set out in the data access request agreement and approval letter.

The RLU will email all pending approval letters from all relevant data stewards along with Data Release Letter to the DARS. **The Administrator** is to save all documents and update the DARTS database.

Academic Research – DAR/PNET



[DATE]

File No. [AMEND NO]

[APPLICANT NAME]
[APPLICANT ADDRESS]
[APPLICANT ADDRESS]
[APPLICANT ADDRESS]
[APPLICANT ADDRESS]

Dear [APPLICANT NAME]:

RE: [AMEND NO #] [PROJECT TITLE]

The Ministry of Health (the “Ministry”) is pleased to approve the amendment request:

- Additional year(s) of data
[INSERT DATA YEARS APPROVED]
- Addition of data file(s) and/or data field(s)
[INSERT DATA FILES/FIELDS APPROVED]
- Addition of external data linkages
[INSERT LINKAGES APPROVED]
- Addition of Project Team Members
[INSERT TEAM MEMBERS APPROVED]
- Extension of data retention date to [DATA RETENTION DATE]
- [OTHER]

All other terms and conditions remain the same as the original Agreement and prior amendment(s).

Use of Data

The Applicant is permitted to use this data for the above project only.

The Applicant must not use, or disclose personal information specified in this Agreement without written authorization of the Ministry.

Retention of Data

The dataset may be retained until [**three years** from the date of the first data release letter from Population Data BC/ **OR DATA RETENTION DATE**]. Upon termination of this Agreement, all data provided to the Applicants must be returned to the Ministry or destroyed in manner consistent with Ministry standards.

Written confirmation of data destruction must be provided to the Ministry.

Any amendment to this Agreement beyond this date requires written approval from the Ministry.

Records of Access and Pledge of Confidentiality

The Applicant will maintain a record of the name of each person who has access to the data and notify the Ministry of any changes. The Applicant is responsible for submitting signed Pledges of Confidentiality for all individuals who have access to study data.

Data Preparation

Please note that Population Data BC processes approved data requests in date order. Given the high volume of requests that are received, your data extract will be prepared as quickly as possible. Questions related to the preparation of your data can be directed to the Research Liaison Unit, Population Data BC, by email at rlu@popdata.bc.ca.

Data Storage & Access

Access to the data via the Secure Research Environment (SRE) at Population Data BC may be made available pending written agreement between the Applicant and Population Data BC. All data including password protected CDs will be kept in a physically secure location pursuant to the application at the time of this approval.

The Applicant is only allowed to access this data from within Canada.

Data Linkage

No other linkages of any kind are to be made without prior written consent from the Ministry. All data will be linked per standard practice.

Audit & Compliance

The Ministry shall have the right to audit the premises and records of the Applicant that are directly related to the Applicant's responsibilities under this Agreement. This includes, but is not limited to, the right to inspect the maintenance of records of access, the security of the data and the specific uses that have been made of the data.

The Applicant agrees to cooperate in this audit.

Ethics

The Applicant is responsible for maintaining current Ethics Research Board approvals at the institutions where data is to be analyzed for the full period that study data is in your possession. Current ethics approval for the above study expires **[ETHICS EXPIRY DATE]**.

Research Outputs

ALL written materials intended for public dissemination as an outcome of the research project must be submitted to the Ministry for review and comment prior to release. The Ministry is committed to providing feedback/comment within 45 days of submission.

- All research outputs must be published at a geographic level no lower than Local Health Area (LHA). Cell size minimum requirements must be met in all publications.
- Electronic submission of written materials is preferred (i.e. MS Word or PDF format).

Documents can be mailed or faxed to:

**Chief Data Steward
Ministry of Health
1515 Blanshard Street
Victoria BC V8W 3C8**

Fax: (250) 952-2002

Sincerely,

Kelly Moran
A/Executive Director
Information Management and Knowledge Services
Health Sector IM/IT Division
Ministry of Health
Province of British Columbia

pc: [Researcher Liaison Unit, Population Data BC, University of British Columbia](#)
[Robert C. Brunham, Provincial Executive Director and Scientific Director, BC Centre for Disease Control](#)
[Jack Shewchuk, Chief Executive Officer, Vital Statistics Agency](#)
[Randy Slemko, Manager, BC Ambulance Service](#)
[Ryan Woods, Scientific Director, BC Cancer Registry](#)
[Melissa Murdock, A/Director, Information Management and Knowledge Services, Ministry of Health](#)
[Kim Williams, Executive Director, Information Systems, Perinatal Services BC](#)
[Lori Guiton, Director, Research Services, WorkSafeBC](#)
[Andrew Kmetec, Provincial Director, Data Services, Evaluation and Research, Cardiac Services BC](#)
[Dr. H.M. Oetter, Registrar, College of Physicians and Surgeons of British Columbia](#)
[Bruce Carleton, Chair, Data Stewardship Committee](#)

Ruth Hershler, Data Steward, Human Early Learning Partnership

[DATE]

File Number: [DAR#]

[APPLICANT NAME]
[APPLICANT ADDRESS]
[APPLICANT ADDRESS]
[APPLICANT ADDRESS]
[APPLICANT ADDRESS]

Dear [APPLICANT NAME]:

RE: [DAR #] [PROJECT TITLE]

The Ministry of Health (the “Ministry”) is pleased to approve access to the following data per the Data Access Request (DAR) **[VERSION]**.

Kindly acknowledge the terms and conditions of this approval by signing and completing the information on the final page and returning it to the Research Liaison Unit at Population Data BC.

Cohort

Cohort: [COHORT DEFINITION]

Control Group: [CONTROL DEFINITION]

Ministry Databases & Date Range

- [DATABASE] [DATE RANGE]

Use of Data

The Applicant is permitted to use this data for research objectives specified in the DAR for the above project only.

No other use or disclosure is permitted without written approval from the Ministry.

Retention of Data

The data may be retained until **three years** from the date of the first data release letter from Population Data BC. Upon termination of this Agreement, all data provided to the Applicants must be returned to the Ministry or destroyed in manner consistent with Ministry standards.

Written confirmation of data destruction must be provided to the Ministry.

Any amendment to this Agreement beyond this date requires written approval from the Ministry.

Records of Access and Pledge of Confidentiality

As per your DAR, the following people are permitted to access data:

- **XXX**

The Applicant is responsible for ensuring that every individual with access to data signs a Pledge of Confidentiality and notifying the Ministry any changes.

Access for additional individuals must be first approved by the Ministry in writing.

Data Preparation

Data will be prepared by Population Data BC. Questions related to the preparation of your data can be directed to the Research Liaison Unit, Population Data BC, by email at rlu@popdata.bc.ca.

Data Storage & Access

As per your DAR, data will be stored on the Secure Research Environment (SRE) at Population Data BC. Any changes to this storage location must be first approved by the Ministry in writing.

The Applicant is only allowed to access data from within Canada.

Data Linkage

Data linkage will be performed by Population Data BC or as outlined in the DAR. No other linkages of any kind are to be made without written approval from the Ministry.

All data will be linked per standard practice.

Audit & Compliance

The Ministry shall have the right to audit the premises and records of the Applicant that are directly related to the Applicant's responsibilities under this Agreement. This includes, but is not limited to, the right to inspect the maintenance of records of access, the security of the data and the specific uses that have been made of the data.

The Applicant agrees to cooperate in this audit.

Ethics

The Applicant is responsible for maintaining current Ethics Research Board approvals at the institutions where data is to be analyzed for the full period that data is in your possession. Current ethics approval for the above study expires **[ETHICS EXPIRY DATE]**.

Research Outputs

ALL written materials intended for public dissemination as an outcome of the research project must be submitted to the Ministry for review and comment prior to release. The Ministry is committed to providing feedback/comment within 45 business days of submission.

- All research outputs must be published at a geographic level no lower than Local Health Area (LHA). Cell size minimum requirements must be met in all publications.
- Electronic submission of written materials is preferred (i.e. MS Word or PDF format)
- Findings resulting from this project must not reveal either directly, indirectly or inadvertently the identities of any individuals, individual communities or hospitals.

Documents must be submitted online:

http://www.popdata.bc.ca/forms/prepublicdisclosure_review

Signatures

Kelly Moran, A/Executive Director
Information Management and Knowledge Services
Ministry of Health

Applicant Signature

Print name

Date

Principal Investigator Signature (if different from Applicant)

Print name

Date

pc: Researcher Liaison Unit, Population Data BC, University of British Columbia
Robert C. Brunham, Provincial Executive Director and Scientific Director, BC Centre for Disease Control
Jack Shewchuk, Chief Executive Officer, Vital Statistics Agency
Randy Slemko, Manager, BC Ambulance Service
Ryan Woods, Scientific Director, BC Cancer Registry
Melissa Murdock, A/Director, Information Management and Knowledge Services, Ministry of Health
Kim Williams, Executive Director, Information Systems, Perinatal Services BC
Lori Gupton, Director, Research Services, WorkSafeBC
Andrew Kmetz, Provincial Director, Data Services, Evaluation and Research, Cardiac Services BC
Dr. H.M. Oetter, Registrar, College of Physicians and Surgeons of British Columbia
Bruce Carleton, Chair, Data Stewardship Committee
Ruth Hersher, Data Steward, Human Early Learning Partnership

[DATE]

File Number: [AMEND/PNET #]

[APPLICANT NAME]
[APPLICANT ADDRESS]
[APPLICANT ADDRESS]
[APPLICANT ADDRESS]
[APPLICANT ADDRESS]

Dear [APPLICANT NAME]:

RE: [AMEND/PNET #] [PROJECT TITLE]

The Data Stewardship Committee is pleased to approve the following amendment request:

- Additional year(s) of data
[INSERT DATA YEARS APPROVED]
- Addition of data file(s) and/or data field(s)
[INSERT DATA FILES/FIELDS APPROVED]
- Addition of external data linkages
[INSERT LINKAGES APPROVED]
- Addition of Project Team Members
[INSERT TEAM MEMBERS APPROVED]
- Extension of data retention date to [DATA RETENTION DATE]
- [OTHER]

All other terms and conditions remain the same as the original Agreement and prior amendment(s).

Use of Data

The Applicant is permitted to use this data for the above project only.

The Applicant must not use, or disclose personal information specified in this Agreement without written authorization of the Data Stewardship Committee.

Retention of Data

The dataset may be retained until [**three years** from the date of the first data release letter from Population Data BC/ **OR DATA RETENTION DATE**]. Upon termination of this Agreement,

all data provided to the Applicants must be returned to the Ministry of Health (the “Ministry”) or destroyed in manner consistent with Ministry standards.

Written confirmation of data destruction must be provided to the Ministry.

Any amendment to this Agreement beyond this date requires written approval from the Data Stewardship Committee.

Records of Access and Pledge of Confidentiality

The Applicant will maintain a record of the name of each person who has access to the data and notify the Ministry of any changes. The Applicant is responsible for submitting signed Pledges of Confidentiality for all individuals who have access to study data.

Data Preparation

Please note that Population Data BC and the Ministry process approved data requests in date order. Given the high volume of requests that are received, your data extract will be prepared as quickly as possible. Questions related to the preparation of your data can be directed to the Research Liaison Unit, Population Data BC, by email at rlu@popdata.bc.ca.

Data Storage & Access

Access to the data via the Secure Research Environment (SRE) at Population Data BC may be made available pending written agreement between the Applicant and Population Data BC. All data including password protected CDs will be kept in a physically secure location pursuant to the application at the time of this approval.

The Applicant is only allowed to access this data from within Canada.

Data Linkage

No other linkages of any kind are to be made without prior written consent from the Ministry. All data will be linked per standard practice.

Audit & Compliance

The Ministry shall have the right to audit the premises and records of the Applicant that are directly related to the Applicant’s responsibilities under this Agreement. This includes, but is not limited to, the right to inspect the maintenance of records of access, the security of the data and the specific uses that have been made of the data.

The Applicant agrees to cooperate in this audit.

Ethics

The Applicant is responsible for maintaining current Ethics Review Board approvals at the institutions where data is to be analyzed for the full period that study data is in your possession. Current ethics approval for the above study expires **[ETHICS EXPIRY DATE]**.

Research Outputs

ALL written materials intended for public dissemination as an outcome of the research project must be submitted to the Ministry for review and comment prior to release. The Ministry is committed to providing feedback/comment within 45 days of submission.

- All publications must be published at a geographic level no lower than Local Health Area (LHA). Cell size minimum requirement must be met in all publications.
- Electronic submission of written materials is preferred (i.e. MS Word or PDF format).

Documents can be mailed or faxed to:

**Data Stewardship Secretariat
Ministry of Health
1515 Blanshard Street
Victoria BC V8W 3C8**

Fax: (250) 952-2002

Sincerely,

Dr. Bruce Carleton, Chair
Data Stewardship Committee

pc: [Researcher Liaison Unit, Population Data BC, University of British Columbia](#)
[Robert C. Brunham, Provincial Executive Director and Scientific Director, BC Centre for Disease Control](#)
[Jack Shewchuk, Chief Executive Officer, Vital Statistics Agency](#)
[Randy Slemko, Manager, BC Ambulance Service](#)
[Ryan Woods, Scientific Director, BC Cancer Registry](#)
[Melissa Murdock, A/Director, Information Management and Knowledge Services, Ministry of Health](#)
[Kim Williams, Executive Director, Information Systems, Perinatal Services BC](#)
[Lori Guiton, Director, Research Services, WorkSafeBC](#)
[Andrew Kmetc, Provincial Director, Data Services, Evaluation and Research, Cardiac Services BC](#)
[Dr. H.M. Oetter, Registrar, College of Physicians and Surgeons of British Columbia](#)
[Kelly Moran, A/Executive Director, Information Management and Knowledge Services, Ministry of Health](#)
[Ruth Hershler, Data Steward, Human Early Learning Partnership](#)

[DATE]

File Number: [DAR/PNET #]

[APPLICANT NAME]
[APPLICANT ADDRESS]
[APPLICANT ADDRESS]
[APPLICANT ADDRESS]
[APPLICANT ADDRESS]

Dear [APPLICANT NAME]:

RE: [DAR/PNET #] [PROJECT TITLE]

The Data Stewardship Committee is pleased to approve access to the following data:

Approved Cohort & Control Group

Cohort: [COHORT DEFINITION].

Control Group: [CONTROL DEFINITION]

- [PHARMANET VARIABLES] [DATE RANGE]

Use of Data

The Applicant is permitted to use this data for the above project only.

The Applicant must not use, or disclose personal information specified in this Agreement without written authorization of the Data Stewardship Committee.

Retention of Data

The dataset may be retained until **three years** from the date of the first data release letter from Population Data BC. Upon termination of this Agreement, all data provided to the Applicants must be returned to the Ministry of Health (the “Ministry”) or destroyed in manner consistent with Ministry standards.

Written confirmation of data destruction must be provided to the Ministry.

Any amendment to this Agreement beyond this date requires written approval from the Data Stewardship Committee.

Records of Access and Pledge of Confidentiality

The Applicant will maintain a record of the name of each person who has access to the data and notify the Ministry of any changes. The Applicant is responsible for submitting signed Pledges of Confidentiality for all individuals who have access to study data.

Data Preparation

Please note that Population Data BC and the Ministry process approved data requests in date order. Given the high volume of requests that are received, your data extract will be prepared as quickly as possible. Questions related to the preparation of your data can be directed to the Research Liaison Unit, Population Data BC, by email at rlu@popdata.bc.ca.

Data Storage & Access

Access to the data via the Secure Research Environment (SRE) at Population Data BC may be made available pending written agreement between the Applicant and Population Data BC. All data including password protected CDs will be kept in a physically secure location pursuant to the application at the time of this approval.

The Applicant is only allowed to access this data from within Canada.

Data Linkage

No other linkages of any kind are to be made without prior written consent from the Ministry. All data will be linked per standard practice.

Audit & Compliance

The Ministry shall have the right to audit the premises and records of the Applicant that are directly related to the Applicant's responsibilities under this Agreement. This includes, but is not limited to, the right to inspect the maintenance of records of access, the security of the data and the specific uses that have been made of the data.

The Applicant agrees to cooperate in this audit.

Ethics

The Applicant is responsible for maintaining current Ethics Review Board approvals at the institutions where data is to be analyzed for the full period that study data is in your possession. Current ethics approval for the above study expires **[ETHICS EXPIRY DATE]**.

Research Outputs

ALL written materials intended for public dissemination as an outcome of the research project must be submitted to the Ministry for review and comment prior to release. The Ministry is committed to providing feedback/comment within 45 days of submission.

- All publications must be published at a geographic level no lower than Local Health Area (LHA). Cell size minimum requirement must be met in all publications.

- Electronic submission of written materials is preferred (i.e. MS Word or PDF format).

Documents can be mailed or faxed to:

**Data Stewardship Secretariat
Ministry of Health
1515 Blanshard Street
Victoria BC V8W 3C8**

Fax: (250) 952-2002

Sincerely,

Dr. Bruce Carleton, Chair
Data Stewardship Committee

pc: Researcher Liaison Unit, Population Data BC, University of British Columbia
Robert C. Brunham, Provincial Executive Director and Scientific Director, BC Centre for Disease Control
Jack Shewchuk, Chief Executive Officer, Vital Statistics Agency
Randy Slemko, Manager, BC Ambulance Service
Ryan Woods, Scientific Director, BC Cancer Registry
Melissa Murdock, A/Director, Information Management and Knowledge Services, Ministry of Health
Kim Williams, Executive Director, Information Systems, Perinatal Services BC
Lori Guiton, Director, Research Services, WorkSafeBC
Andrew Kmetc, Provincial Director, Data Services, Evaluation and Research, Cardiac Services BC
Dr. H.M. Oetter, Registrar, College of Physicians and Surgeons of British Columbia
Kelly Moran, A/Executive Director, Information Management and Knowledge Services, Ministry of Health
Ruth Hershler, Data Steward, Human Early Learning Partnership

Below is a copy of the online Pre-Publication Submission form on the Population Data BC website. The online form can be found at http://www.popdata.bc.ca/forms/prepublicdisclosure_review

SUBMISSION FORM for the PRE-PUBLIC DISCLOSURE REVIEW OF RESEARCH MATERIALS

In signing a Research Agreement with a public body for access to data, researchers commit to sending Research Materials to the public body in advance of public dissemination. Data Stewards, as those responsible for ensuring appropriate uses of the public body's data, check that: privacy / confidentiality requirements are upheld; there is no gross misuse of the data; and that the data is appropriately referenced.

PLEASE READ BEFORE SUBMITTING

1. Your Research Agreement requires that you provide Data Stewards 45 DAYS to review your submission.
2. Submissions that have been previously vetted in a different publication format and do not use new data and/or analysis DO NOT require further vetting (PopData and Data Stewards still request that copies be provided).
3. Presentation of research materials to colleagues DO NOT require approval (see: www.popdata.bc.ca/dataaccess/process/dsreviewreqs for the definition of colleague; PopData and Data Stewards still request that copies be provided).

Further information on the research material review requirements can be found at:

www.popdata.bc.ca/dataaccess/process/dsreviewreqs

Please note: Population Data BC will submit the Research Materials for review to **all** relevant Data Stewards, including the Ministry of Health, on your behalf. If you prefer, you may submit directly to the Ministry of Health at ResearchDataAccessServices@gov.bc.ca and copy RLU@popdata.bc.ca.

Please complete the form below for each item of Research Material which is being submitted for review.

Project number: *

Contact name: *

Contact email: *

Project title: *

Type of Research Material for public disclosure

Type of material: *

- ☐ Conference abstract
- ☐ Presentation of research materials (posters, seminars, lectures, etc.)
- ☐ Article for general public release (newspaper/magazine/blog/wiki etc.)
- ☐ Op-ed for general public release (newspaper/magazine/blog/wiki etc.)
- ☐ Journal publication
- ☐ Academic thesis or dissertation material
- ☐ Interview (radio, television, internet, etc.)
- ☐ Instructional use (examples in lectures and/or lab exercises, etc.)

Other, please describe:

Please list all databases relevant to this publication (e.g., MSP, VSA):

Names of authors: *

Names of authors who have access to the data released under this project: *

Title of publication: *

Please describe how this publication ties to/supports the objectives of this project: *

Please attach file:

Has this Research Material already been delivered/published?: *

- ☐ Yes
- ☐ No

If you would like to include additional information (such as details of the journal to which you are submitting or the event at which you are making your Research Material public) please do so here:

Please confirm the following:

I confirm that the attached document is the final draft to be submitted for publication: *

- ☐ Yes

I understand that Data Stewards require notification of any pre-publication changes made to this document and a copy of the final publication: *

- ☐ Yes

I confirm that this publication does not contain any risk of re-identification of an individual (e.g., small cell sizes, small geographic areas): *

- ☐ Yes

I confirm that all relevant databases are properly referenced (e.g., MSP, DAD): *

- ☐ Yes

For more information on correctly referencing databases please visit:

<http://www.popdata.bc.ca/dataaccess/process/referencing>

Submit

Project Summary

Project Number-Title:
Primary Investigator(s):
Research Team Member(s):
Funding:
Ethics Board/Expiration:
Data Storage:
MoH Date of Receipt:

BRIEF Project Description / Project Objectives

Please insert a brief project description

Project Objectives:

Please insert project objectives in bullet form

Public Health Benefits – Statement

Please insert a brief statement on how this research benefits public health

Cohort Definition / Control Group (as applicable)

Please insert the cohort/control group definition including the name of the database that will be used to create the cohort/control group

Databases

Databases at Popdata Holdings: (Please insert years (fiscal/calendar))

- Name of database (Approval received Month day, year)

Databases External to Popdata Holdings: (Please insert years (fiscal/calendar))

- Name of database (Approval received Month day, year)

Geographic Fields (e.g. LHA)

Please list all Geographic fields that are requested on the Consolidation checklist in bullet form

Potential Risk(s) / Mitigation (e.g. cell size)

Risk: *Please insert a brief description of what the risk is*

Researcher's Rationale:

Please insert a summary of rationale provided by the researcher, as applicable

Mitigation:

Please list all mitigation strategies in bullet form

Conditions for release

- N/A

If there are any project specific approval conditions not captured in the DAR, please list in bullet form and make sure that the same conditions appear on the MoH approval letter.

Recommendation

- To submit for approval



Submit this completed form to the email address:
healthdatacentral@gov.bc.ca

Questions about the request process or any part of this application may be directed to the email address above.

MINISTRY OF HEALTH USE ONLY

File Number

Date Received

PROJECT TITLE

RELATIONSHIP TO PREVIOUS AGREEMENT(S) / PREVIOUS REQUESTS

In cases where a relationship exists between this request and a previous agreement with the Ministry of Health, or a previously approved data extract from the Ministry of Health, provide the file number(s).

Data Request File Number (if known)

☐ Existing agreement attached

Briefly describe the relationship between this data request and previous agreement(s) / previous requests.

SUPPORTING DOCUMENTATION

SUPPORTING DOCUMENTS

Electronic copies of supporting documentation attached to the request. Check as applicable.

- ☐ Funding Agreement
- ☐ Privacy Impact Assessment (PIA)
- ☐ Security and Threats Risk Assessment (STRA)
- ☐ Transfer Under Agreements (or other project-related contracts)
- ☐ General Services Agreement
- ☐ Other (specify)

SECTION I: REQUESTOR INFORMATION

REQUESTOR (Person that will be responsible for the Data)

LAST NAME		FIRST NAME		TITLE	
POSITION			INSTITUTION NAME		
STREET ADDRESS			CITY	PROV	POSTAL CODE
PHONE	FAX		EMAIL		

INSTITUTION ADDRESS (if different from applicant address, e.g., University, Health Authority, Ministry)

STREET ADDRESS			CITY	PROV	POSTAL CODE
PHONE	FAX		EMAIL		

SIGNATORY TO AGREEMENT (if different from the Requestor)

The party accountable for enforcing the terms and conditions of the agreement

LAST NAME		FIRST NAME		TITLE	
POSITION			INSTITUTION NAME		
STREET ADDRESS			CITY	PROV	POSTAL CODE
PHONE	FAX		EMAIL		

PROJECT MANAGER (primary contact person for correspondence, if different from requestor)

LAST NAME		FIRST NAME		TITLE	
POSITION			INSTITUTION NAME		
STREET ADDRESS			CITY	PROV	POSTAL CODE
PHONE	FAX		EMAIL		

PERSONS WHO WILL HAVE ACCESS TO THE DATA

Identify ALL individuals who will have access to the requested data AT ANY TIME. Attach a separate sheet if necessary.

NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION
NAME	POSITION	INSTITUTION

SECTION II: PROJECT DESCRIPTION

BACKGROUND

Please include public interest value statement and how it relates to this application. If conducting a program evaluation, name and describe the program.

PROJECT PURPOSE

Please ensure the project objectives are clearly related to the data request.

SMALL CELL SIZE

If you anticipate that small cell size will be an issue for your project (e.g., there are fewer than five individuals in a geographic area, in a specified age group or with the same laboratory results), please describe measures that will be taken to protect confidentiality during analysis and in any publication or distribution of results.

SECTION III: PROJECT SPONSOR (IF APPLICABLE)

MINISTRY OR OTHER FUNDING

Please indicate direct or indirect sources – e.g , grant funding agency, Ministry sponsored, etc.

SECTION IV: DATA SECURITY AND ACCESS

DATA TRANSFER

Please indicate the preferred method of data transfer

- ☐ Secure File Transfer Protocol (Ministry of Health default option)
- ☐ Encrypted CD (double envelope and separate password)

NOTE: Data and derived information, other than aggregated information such as statistical output, must be transferred by courier; in person by someone named above as having access to the data; or by secure file transfer as approved by the ministry.

E-mail, regular mail and fax are not acceptable transfer methods at any time.

PHYSICAL LOCATION

Indicate the physical locations(s) where data will be used or accessed, including research sites, and storage sites (if different). Indicate all general physical security measures in place at each location. Include measures taken to protect workstations, hard copy and source media.

LOCATION 1

LAST NAME		FIRST NAME		TITLE	
STREET ADDRESS		CITY		PROV	POSTAL CODE
PHYSICAL SECURITY METHODS <input type="checkbox"/> LOCKED FILE CABINET <input type="checkbox"/> DOOR KEYPAD <input type="checkbox"/> OTHER (SPECIFY)					

LOCATION 2

LAST NAME		FIRST NAME		TITLE	
STREET ADDRESS		CITY		PROV	POSTAL CODE
PHYSICAL SECURITY METHODS <input type="checkbox"/> LOCKED FILE CABINET <input type="checkbox"/> DOOR KEYPAD <input type="checkbox"/> OTHER (SPECIFY)					

NOTE: All physical locations housing data must be locked, except when an individual authorized to access the data is present.

Describe how, and from where, any regular maintenance and backups of your network are conducted, where backup material is stored, and backup retention schedule.

NETWORK SECURITY AND BACKUPS

If data will be stored on a network or system to which individuals other than identified project personnel have access, or on a system connected to a public network (the internet), indicate and describe, the network security measures in place.

Location 1

- ☐ Firewall
- ☐ Password changed every _____ days
- ☐ Password rules (minimum length, complexity)
- ☐ Drives or folders with access restricted to persons listed in Section 1
- ☐ Health Data File encryption
- ☐ List the encryption-in-transport protocol used for accessing the health data file from a remote PC:

- ☐ Assuming health data file is encrypted, where is key stored, and is key store management documented?

- ☐ Other: _____
- ☐ Security audit: _____
- ☐ Access tracking: _____

Describe how, and from where, any regular maintenance and backups of your network are conducted, where backup material is stored, and backup retention schedule.

Location 2

- ☐ Firewall
- ☐ Password changed every _____ days
- ☐ Password rules (minimum length, complexity)
- ☐ Drives or folders with access restricted to persons listed in Section 1
- ☐ Health Data File encryption
- ☐ List the encryption-in-transport protocol used for accessing the health data file from a remote PC:

- ☐ Assuming health data file is encrypted, where is key stored, and is key store management documented?

- ☐ Other: _____
- ☐ Security audit: _____
- ☐ Access tracking: _____

Describe how, and from where, any regular maintenance and backups of your network are conducted, where backup material is stored, and backup retention schedule.

PERSONAL COMPUTER SECURITY AND BACKUPS

If data will be accessed or stored on the hard drive of a personal computer, identify all security measures taken to protect data residing on the PC.

Location 1

- ☐ Electronic locking system
- ☐ Logon password
- ☐ Individual file or folder passwords
- ☐ If you use local storage of the health data file, are the files encrypted? _____
- ☐ Removable drives
- ☐ Physical attachment to floor or object
- ☐ Software firewall (describe): _____
- ☐ Antivirus (describe): _____
- ☐ Antispyware or adware (describe): _____
- ☐ If you use remote server storage for your health data, is there a policy forbidding local storage of the health data on the PC documented, trained and audited? ☐ Yes ☐ No
- ☐ If you use remote server storage for your health data, is there documented policy enforcing the use of encryption-in-transport (as documented in the section network security earlier in this form)? ☐ Yes ☐ No
- ☐ Other (describe): _____

Location 2

- ☐ Electronic locking system
- ☐ Logon password
- ☐ Individual file or folder passwords
- ☐ If you use local storage of the health data file, are the files encrypted? _____
- ☐ Removable drives
- ☐ Physical attachment to floor or object
- ☐ Software firewall (describe): _____
- ☐ Antivirus (describe): _____
- ☐ Antispyware or adware (describe): _____
- ☐ If you use remote server storage for your health data, is there a policy forbidding local storage of the health data on the PC documented, trained and audited? ☐ Yes ☐ No
- ☐ If you use remote server storage for your health data, is there documented policy enforcing the use of encryption-in-transport (as documented in the section network security earlier in this form)? ☐ Yes ☐ No
- ☐ Other (describe): _____

NOTE: Storage of data on laptops, notebooks, handheld devices and other portable devices (e.g. external memory) will not be permitted.

SECTION V: DATA REQUEST

COHORT DEFINITION / POPULATION OF INTEREST

Please provide a detailed text description of your study population including date ranges. Describe which databases and variables will be used to define your population of interest (e.g. all women in BC diagnosed with breast cancer between April 1, 2000 and March 31, 2010 in the BC Cancer Registry database).

MINISTRY OF HEALTH DATA

Please indicate the Ministry of Health databases relevant to this data request.

- ☐ Discharge Abstracts Database
- ☐ Medical Services Plan payment information
- ☐ Home and Community Care
- ☐ Mental Health Services
- ☐ PharmaNet
- ☐ PharmaCare
- ☐ Other (specify): _____

For access to each of the requested Ministry of Health databases, please submit the corresponding data variable checklist along with this application. These checklists will assist the program area in preparing your data extract. Checklists can be downloaded from the Health Data Central website at <https://www.health.gov.bc.ca/exforms/data.html>.

DATA LINKAGE

Do you intend to link Ministry of Health databases to any external sources (i.e. data sources not held by the Ministry)?

- ☐ YES → please attach any Agreements, Memorandums of Understanding (MOUs), etc. pertaining to use of external databases as supporting documentation
- complete Section VI: Linkage to External Data Source
- ☐ NO

SECTION VI: LINKAGE TO EXTERNAL DATA SOURCE

This Section is designed to capture detailed information pertaining to LINKAGE of requested Ministry of Health data to external data sources (i.e. linking distinct data sources using a linkage key such as Personal Health Number (PHN)).

PART 1 - LINKAGE KEY TABLE

Please complete this Linkage Key Table to indicate all linkage keys that are required to facilitate linkage (e.g. Personal Health Number (PHN), Full Date of Birth, First Name, Last Name, etc.).

Data Source	Field Name	Use for Linkage (Y/N)	Retain for Analysis (Y/N)	Rationale if requesting retention for analysis

Sample

Data Source	Field Name	Use for Linkage (Y/N)	Retain for Analysis (Y/N)	Rationale if requesting retention for analysis
BC Cancer Registry	PHN	Y	Y	

PART 2 - EXTERNAL DATA VARIABLES FOR ANALYSIS

Do you intend to link the requested Ministry of Health databases to any external data variables for analysis?

- ☐ YES → please attach a list of all external data variables and their sources, including date
- ☐ NO

PART 3 - LINKAGE STRATEGY

Please select one of the following linkage strategies.

- ☐ **Cohort defined using External Data Source** – Linkage Strategy A
<https://www.health.gov.bc.ca/exforms/datastewardship/LinkageStrategyA.pdf>
- ☐ **Cohort defined using Ministry of Health Data** – Linkage Strategy B for trusted partners (i.e. health authorities, other ministries)
<https://www.health.gov.bc.ca/exforms/datastewardship/LinkageStrategyB.pdf>
- ☐ **Others** – Please describe the proposed linkage strategy in details. Include a flow chart if available.



Submit this completed form to the email address:
healthdatacentral@gov.bc.ca

Questions about the request process or any part of this application may be directed to
the email address above.

MINISTRY OF HEALTH USE ONLY

File Number

Date Received

PROJECT TITLE

APPLIES TO COHORT(S)

DATE RANGE

From (yyyy/mm/dd)

To (yyyy/mm/dd)

DISCHARGE ABSTRACTS DATABASE – HOSPITAL SEPARATIONS (April 1, 1991 onwards)

Includes discharges, transfers and deaths of in-patients from acute care hospitals in BC, including day surgeries. Fields are available in all years unless otherwise noted. Note: Files are grouped into fiscal years by separation date, not the date of admission. Abortion procedures, including those conducted in concert with other procedures, are unavailable from all applicable files. This is in accordance with BC Freedom of Information and Protection of Privacy Act.

DATA VARIABLES	DEFINITION
<input type="checkbox"/> Client Study ID Project-specific identification number	Study identification number
<input type="checkbox"/> Client Gender	Patient's gender
<input type="checkbox"/> Date of birth (YYYYMM)	Birth date of patient (Year/Month only)
<input type="checkbox"/> Client HA	Health Authority
<input type="checkbox"/> Client HSDA	Health Service Delivery Area
<input type="checkbox"/> Client Local Health Area Code (LHA 3)	The Local Health Area (LHA) is the smallest geographical unit of analysis and is based on the postal code of the patient. The LHA is derived from the Translation Master File (TMF) for valid BC postal codes only.
<input type="checkbox"/> Client FSA	Forward Sortation Area
<input type="checkbox"/> Other Client Geographical Information	Other geographical divisions from Statistics Canada (i.e. CMA, CSD, CD) could be requested, as well as researcher defined geographical units.
<input type="checkbox"/> BC hospital number – Replaced by project-specific identification number, OR	

DATA VARIABLES	DEFINITION
<input type="checkbox"/> BC hospital number (unencrypted) (HOSP) – Rationale describing why this field is required must be supplied before it will be considered for release:	
<input type="checkbox"/> Level of care	Indicates the level of care provided to the patient.
<input type="checkbox"/> Admission date	The date the patient was admitted to the facility.
<input type="checkbox"/> Admission time (hour only up to 2000/01, from 2001/02 onwards, complete time is available)	The time of day the patient was admitted to the facility.
<input type="checkbox"/> Discharge date	The date the patient was separated (discharged) from the facility.
<input type="checkbox"/> Discharge (separation) time - (hour only up to 2000/01, from 2001/02 onwards, complete time is available)	The time of day the patient was separated (discharged) from the facility.
<input type="checkbox"/> Admit category	This indicates the urgency of admission.
<input type="checkbox"/> Ambulance flag	This is a flag that indicates if a patient arrive by ambulance
<input type="checkbox"/> Ambulance type	If the patient was brought to the facility by ambulance, this code indicates the type of ambulance used
<input type="checkbox"/> Readmission code (01/02 onward)	Denotes a readmission to the acute care unit of the same reporting facility. The focus of the field is whether the readmission was unplanned
<input type="checkbox"/> Entry code (91/92 onward)	The patient's type or mode of entry to a facility
<input type="checkbox"/> Exit code (91/92 – 00/01)	The patient's type or mode of exit from a facility
<input type="checkbox"/> Autopsy (91/92 – 00/01)	This code indicates if an autopsy was performed.
<input type="checkbox"/> Coroner (91/92 – 00/01)	This code indicates if a coroner/Medical Examiner was involved following a patient death.
<input type="checkbox"/> Operative death code (91/92 – 00/01)	This code indicates the type of patient's death related to an operative procedure.
<input type="checkbox"/> Supplemental death code (91/92 – 00/01)	This code identifies the type of patient's death
<input type="checkbox"/> Discharge (separation) disposition (01/02 onward)	Status of patient upon leaving hospital
<input type="checkbox"/> Death in OR indicator (01/02 onward)	Code denotes the Patient's Death occurred in an operating room /intervention location or during recovery in the post-anesthetic recovery room
<input type="checkbox"/> Death in special care unit indicator (01/02 onward) (SCUDEATH)	Code to indicate death in a Special Care Unit
<input type="checkbox"/> Acute/rehab days	A calculated value for the number of days spent in Acute and Rehab levels only
<input type="checkbox"/> Alternate level of care (ALC) length of stay	An ALC patient has finished the acute care phase of treatment but remains in an acute care bed waiting placement in an extended care unit, nursing home, etc.

DATA VARIABLES	DEFINITION
<input type="checkbox"/> Chronic behaviour disorder unit days	Number of days associated with patient service
<input type="checkbox"/> Discharge planning unit (DPU) days (91/92 – 00/01)	A 3 digit numeric field containing the number of days the patient spent in discharge planning unit.
<input type="checkbox"/> Intensive care unit days	Number of days spent in Intensive Care Unit
<input type="checkbox"/> Rehabilitation days	The number of days spent in the rehabilitation care unit in an Acute Care Hospital (level=A). This value is obtained from the days associated with Patient Service and is not applicable to free standing rehabilitation units (level=R)
<input type="checkbox"/> Total length of stay	The total number of days the patient was hospitalized
<input type="checkbox"/> Length of stay group 1 (91/92 – 06/07)	The length of stay is the total number of days from admission to discharge. The length of stay is then classified into ranges. Group 1 has 21 divisions
<input type="checkbox"/> Length of stay group 2 (91/92 – 06/07)	The length of stay is the total number of days from admission to discharge. The length of stay is then classified into ranges. Group 2 has 12 divisions
<input type="checkbox"/> Hospital size (91/92 – 06/07)	Identifies and groups hospitals according to their bed capacity
<input type="checkbox"/> BC hospital number transferred from – Replaced by project-specific identification number, OR	
<input type="checkbox"/> BC hospital number transferred from – Rationale describing why this field is required must be supplied before it will be considered for release:	
<input type="checkbox"/> BC Hospital number transferred to - Replaced by project-specific identification number	
<input type="checkbox"/> BC Hospital number transferred to Rationale describing why this field is required must be supplied before it will be considered for release:	
<input type="checkbox"/> Level from (91/92 to 00/01)	A code identifying the level of care of the facility from which the Patient was transferred
<input type="checkbox"/> Level to (91/92 to 00/01)	A code identifying the level of care of the Facility to where the Patient was transferred
<input type="checkbox"/> BC care level from (01/02 – onward)	Indicates the care level transferred from. Values in this field differ from those reported in LEVELFROM
<input type="checkbox"/> BC care level to) (01/02 – onward)	Indicates the care level transferred to. Values in this field differ from those reported in LEVELTO
<input type="checkbox"/> Service transfer sub-service (subserv 1-3) (91/92 onward)	A code which further defines the Patient Service Transfer
<input type="checkbox"/> Service transfer days (1 to 3) (91/92 onward)	The Number of days associated with a patient service which is not determined to be the main patient service.
<input type="checkbox"/> Main patient service	Based on the most responsible diagnosis code and is not necessarily the first service that the patient was assigned to

DATA VARIABLES	DEFINITION
<input type="checkbox"/> Patient service group (91/92 – 06/07)	Patient Services Group is based on main patient service, age in years and the first procedure
<input type="checkbox"/> Provider 1 (most responsible physician) (RESPPHYS) Replaced by project-specific identification number	Provider who was most responsible for the Patient's care during hospitalization
<input type="checkbox"/> Provider 1 (most responsible physician) service [Note: Not the same as registered specialty]	A code which identifies the Training or Specialty of the Provider responsible for the Patient's care during hospitalization.
<input type="checkbox"/> Diagnosis codes (max. 16 (ICD9 codes) for 91/92 – 00/01; max 25 (ICD10-CA codes) for 01/02 – forward) (Note: - must be used with diagnosis type, below)	ICD9 diagnosis codes (1-16) available for 91/92 - , ICD10-CA diagnosis codes (1-25) available for 01/02 forward
<input type="checkbox"/> Diagnosis type (max. of 16 for 91/92 – 00/01; 25 for 01/02 onward)	A code which determines the relationship of the diagnosis to the patient's hospitalization
<input type="checkbox"/> Diagnostic short list (based on ICD9 coding) (91/92 – 06/07)	Diagnostic short code
<input type="checkbox"/> Diagnostic short code (based on ICD10-CA coding) (01/02 onward)	Diagnostic short code
<input type="checkbox"/> Pre-admit co-morbidity (-first diagnosis type 1 based on ICD9 coding) (91/92 – 06/07)	Indicates a condition arising at the beginning of the hospital's observation and/or treatment which influences the patient's length of stay and/or significantly influences the management/treatment of the patient while in hospital
<input type="checkbox"/> First E-code (cause of injury) (ICD9 for 91/92 – 00/01; ICD10-CA for 01/02 forward)	This is the first occurrence of an ecode indicating the cause of injury.
<input type="checkbox"/> Second E-code (cause of injury) (ICD9 for 91/92 – 00/01; ICD10-CA for 01/02 forward)	This is the second occurrence of an ecode indicating the second cause of injury.
<input type="checkbox"/> ICD10-CA injury code (01/02 onward)	Identifies the first ICD10-CA injury code on a record (if 7) applicable
<input type="checkbox"/> Procedure code (CCP) (max. of 10 in 91/92 – 00/01; and 20 in 01/02 – 06/07)	CCP procedure codes, converted from CCI Intervention codes (icode1-20)
<input type="checkbox"/> Intervention code (CCI) (max. of 20 codes) (01/02 onward)	Identifies an intervention that is performed during the patient's stay. Must be a valid CCI (Canadian Classification of Health Interventions) code
<input type="checkbox"/> Procedure on admission day indicator	Field name originates from "same day surgery" and indicates that an intervention (not necessarily surgery) was performed on the day of admission
<input type="checkbox"/> Procedure / intervention date (max. of 10 in 91/92 – 00/01; and 20 in 01/02 onward)	The date on which the intervention episode was begun
<input type="checkbox"/> Procedure / intervention time (max. of 20 codes) (09/10 onward)	The time at which the intervention episode was begun
<input type="checkbox"/> Procedure short list (based on CCP coding) (91/92 – 00/01)	Procedure Group. This field name originates from "surgical short list", and is a grouping based on intervention codes

DATA VARIABLES	DEFINITION
<input type="checkbox"/> Intervention short list (based on CCI coding) (01/02 onward)	Intervention Short List.
<input type="checkbox"/> Intervention provider (procedure surgeon) (max. of 10 in 91/92 – 00/01; and 20 in 01/02 onward) Replaced by project-specific identification number	Indicates the Practitioner Number used to identify principal Provider associated with the performed intervention.
<input type="checkbox"/> Procedure surgeons' service (max. of 10 in 91/92 – 00/01; and 20 in 01/02 onward)	Procedure surgeon service [01-99, ZZ, blank] identifies the training specialty of the doctor. This is taken from the CIHI list of physician services. The procedure surgeon service is initialized to 0 if this information is not available
<input type="checkbox"/> Intervention (procedure) anaesthetist (max. of 10 in 91/92 – 00/01; and 20 in 01/02 onward) Replaced by project-specific identification number	Indicates the Practitioner Number of the Anaesthetist associated with the performed intervention.
<input type="checkbox"/> Intervention (procedure) anaesthetic (max. of 10 in 91/92 – 00/01; and 20 in 01/02 onward)	Indicates the type of anaesthesia used during an intervention
<input type="checkbox"/> Operation group 1 (1st procedure) (91/92 – 06/07)	Groupings of procedure based on the first procedure.
<input type="checkbox"/> Operation group 2 (2nd procedure) (91/92 – 06/07)	Groupings of procedures on the second procedure.
<input type="checkbox"/> Operation group 3 (3rd procedure) (91/92 – 06/07)	Groupings of procedures based on the third procedure.
<input type="checkbox"/> Physiotherapy (91/92 – 00/01)	Indicates if the patient received physiotherapy. The data element for physiotherapy indicates if the patient received treatment. It is mandatory to enter code in this field in BC.
<input type="checkbox"/> Occupational therapy (91/92 – 00/01)	Indicates if the patient received occupational therapy. The data element for occupational therapy indicates whether the patient received occupational therapy. It is mandatory to enter code in this field in BC.
<input type="checkbox"/> Tertiary code 1 (93/94 – 00/01)	Tertiary code
<input type="checkbox"/> Tertiary code 2 (93/94 – 00/01)	Tertiary project
<input type="checkbox"/> Mother listed on newborn record (97/98 onward) Replaced by project-specific identification number	A cross-reference filed which records the Mother's chart number (patnum) on the Newborn abstract and the Newborn's chart
<input type="checkbox"/> Gestational age (94/95 – 06/07)	The gestational age is recorded in weeks. It is mandatory on all newborn and obstetrics delivered case and optional on therapeutic abortion cases
<input type="checkbox"/> Infant birth weight	Infant birth weight in grams. Captured for newborns and neonates (age<29 days) only
<input type="checkbox"/> Neonatal Intensive Care Unit Level 2 days (93/94 – onward)	Number of days spent in the Neonatal Intensive Care Nursing Unit Level 2
<input type="checkbox"/> Neonatal Intensive Care Unit Level 3 days (93/94 – onward)	Number of days spent in Neonatal Intensive Care Unit Level 3
<input type="checkbox"/> Medical Intensive Care Nursing Unit days (01/02 – onward)	The number of days spent in a medical intensive care nursing unit
<input type="checkbox"/> Surgical Intensive Care Nursing Unit days (01/02 – onward)	Number of days spent in the Surgical Intensive Care Nursing Unit
<input type="checkbox"/> Trauma Intensive Care Nursing Unit days (01/02 – onward)	Number of days spent in the Trauma Intensive Care Nursing Unit

DATA VARIABLES	DEFINITION
<input type="checkbox"/> Combined Medical/Surgical Intensive Care Nursing Unit days (01/02 – onward)	Number of days spent in combined Medical/Surgical
<input type="checkbox"/> Burn Intensive Care Nursing Unit days 01/02 – onward)	Number of days spent in Burn Intensive Care Nursing Unit
<input type="checkbox"/> Cardiac Intensive Care Nursing Unit days (01/02 – onward)	Number of days spent in Cardiac Intensive Care Nursing Unit
<input type="checkbox"/> Coronary Intensive Care Nursing Unit days	Number of days spent in Coronary Intensive Care Nursing Unit
<input type="checkbox"/> Neonatal Intensive Care Nursing Unit days (01/02 – onward)	Number of days spent in the Neonatal Intensive Care Nursing Unit
<input type="checkbox"/> Neurosurgery Intensive Care Nursing Unit days (01/02 – onward)	Number of days spent in the Neurosurgery Intensive Care Nursing Unit
<input type="checkbox"/> Pediatric Intensive Care Nursing Unit days (01/02 – onward)	Number of days spent in the pediatric intensive care nursing unit
<input type="checkbox"/> Respiriology Intensive Care Nursing Unit days (01/02 – onward)	Number of days spent in Respiriology Intensive Care Nursing Unit
<input type="checkbox"/> Step-down Medical Unit days (01/02 – onward)	Number of days spent in the Step-down Medical Unit
<input type="checkbox"/> Combined Medical /Surgical Step Down Unit days (01/02 onward)	Number of days spent in the Step-down Medical Unit and Number of days spent in the Step-down Surgical Unit
<input type="checkbox"/> Province issuing health care number (91/92 – onward)	Is recorded in conjunction with the Health Care Number
<input type="checkbox"/> Institution number for out of province facilities (91/92 – onward)	Identification number unique to each Province/Territory
<input type="checkbox"/> Province code (location of hospital) (91/92 – onward)	Identifies the province in which the hospital is located
<input type="checkbox"/> Responsibility for payment	Identifies the party responsible for a patient's hospitalization payment
<input type="checkbox"/> Third party liability form	Indicates when a third party liability form has been prepared for the recovery of health care costs by the Ministry of Health

CIHI CMG WITH COMPLEXITY GROUPER VARIABLES/DAY PROCEDURES GROUP

DATA VARIABLES	DEFINITION
<input type="checkbox"/> CIHI case mix group (CMG) (91/92 – 00/01)	Labels for Case Mix Groups assigned by CIHI using the discharge year's grouper.
<input type="checkbox"/> CIHI major clinical category (MCC) (91/92 – 00/01)	Dimension for the Major Clinical Category designating the body system assigned to the case by the CIHI CMG Complexity grouper
<input type="checkbox"/> CIHI CMG age category (91/92 – 00/01)	The Age Category from the event data, based on the CIHI CMG grouping methodology
<input type="checkbox"/> CIHI CMG complexity grade list indicator (91/92 – 00/01)	Grade List (e.g., medical/surgical partition) used in CMG assignment.
<input type="checkbox"/> CIHI CMG complexity/ co-morbidity level (91/92 – 00/01)	Complexity Level assigned to hospitalizations (a CMG-related variable).
<input type="checkbox"/> CIHI expected length of stay (ELOS) (91/92 – 00/01)	Expected Length of Stay based on the CIHI CMG grouping methodology
<input type="checkbox"/> CIHI resource intensity weighting (RIW) value (91/92 – 00/01)	Inpatient weighting value assigned to the case by the CIHI CMG grouper
<input type="checkbox"/> CIHI resource intensity weighting (RIW) exclusion indicator / atypical code (91/92 – 00/01)	CMG Plus RIW Atypical Code

DATA VARIABLES	DEFINITION
<input type="checkbox"/> CIHI day procedure group (DPG) (91/92 – 06/07)	Day Procedure Groups assigned by CIHI using the discharge year's grouper.
<input type="checkbox"/> CIHI day procedure group (DPG) weight (91/92 – 06/07)	Day Procedure weighting value assigned to the case by the CIHI CMG Complexity grouper
<input type="checkbox"/> methodology version (01/02 – onward)	Version number of the CIHI CMG Plus grouper within the methodology year
<input type="checkbox"/> methodology year (01/02 – onward)	Year for which the CIHI CMG Plus grouping methodology was developed
<input type="checkbox"/> major clinical category (MCC+) (01/02 onward)	Dimension for the Major Clinical Category designating the body system assigned to the case by the CIHI CMG Complexity grouper
<input type="checkbox"/> case mix group (CMG+) (01/02 – onward)	Labels for Case Mix Groups assigned by CIHI using the discharge year's grouper.
<input type="checkbox"/> MCC partition (01/02 – onward)	Whether the case is partitioned into intervention or diagnosis partition CMG, based on the presence or absence of interventions
<input type="checkbox"/> Comorbidity level (01/02 – onward)	Complexity Level assigned to hospitalizations (a CMG-related variable).
<input type="checkbox"/> Comorbidity –factor (01/02 – onward)	The cumulative percentage increase on patient cost associated with all comorbidity codes for a particular case using the CIHI CMG Plus grouping methodology
<input type="checkbox"/> CMG age category (01/02 – onward)	Age Category from the event data, based on the CIHI CMG Complexity grouping methodology
<input type="checkbox"/> Flagged intervention count (01/02 – onward)	Flagged Intervention Count Code, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Intervention event count (01/02 – onward)	Intervention Event Count Code, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Intervention OOH count (01/02 – onward)	Intervention Out Of Hospital Count, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> CMG intervention (01/02 – onward)	Intervention Code, if any, that was used to determine the CMG assignment by the CIHI CMG Plus grouping methodology
<input type="checkbox"/> CMG intervention status (01/02 – onward)	Intervention Status (nature of the intervention), based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> CMG intervention location (01/02 – onward)	Intervention Location (site of the intervention), based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> CMG intervention extent (01/02 – onward)	Intervention Extent (scope of the intervention), based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> CMG intervention episode (01/02 – onward)	A number which identifies the intervention episode, if any, that was used to determine the CMG assignment using the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Diagnosis used for CMG assignment (01/02 – onward)	Diagnosis used for CMG assignment by the CIHI CMG Plus grouper
<input type="checkbox"/> Day procedure group (DPG+) (07/08 – _10/11)	Day Procedure Groups assigned by CIHI using the discharge year's grouper.
<input type="checkbox"/> DPG RIW+ (07/08 – 10/11)	DPG Weight for inpatient cases if surgery could have been done as Day Surgery, based on the CIHI CMG Plus grouping methodology

DATA VARIABLES	DEFINITION
<input type="checkbox"/> Inpatient RIW+ (01/02 – onward)	Inpatient weighting value assigned to the case by the CIHI CMG Plus grouper
<input type="checkbox"/> Elos days (01/02 – onward)	Expected Length of Stay based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Inpatient RIW atypical code (01/02 – onward)	CMG Plus RIW Atypical Code
<input type="checkbox"/> Inpatient resource intensity level (01/02 – onward)	CMG Plus resource intensity level
<input type="checkbox"/> Inpatient resource intensity factor (01/02 – onward)	Flagged Intervention Total Resource Intensity Factor, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Trim days (01/02 – onward)	Trim Days, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Cardioversion flag (01/02 – onward)	Flagged Intervention Cardioversion Flag, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Cell saver flag (01/02 – onward)	Flagged Intervention Cell Saver Flag, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Chemotherapy flag (01/02 – onward)	Flagged Intervention Chemotherapy Flag, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Dialysis flag (01/02 – onward)	Flagged Intervention Dialysis Flag, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Heart resuscitation flag (01/02 – onward)	Flagged Intervention Heart Resuscitation Flag, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Mechanical ventilation ge 96 hours flag (01/02 – onward)	Flagged Intervention mechanical ventilation greater than or equal to 96 hours flag, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Mechanical ventilation lt 96 hours flag (01/02 – onward)	Flagged intervention mechanical ventilation less than 96 hours flag, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Feeding tube flag (01/02 – onward)	Flagged Intervention Feeding Tube Flag, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Paracentesis flag (01/02 – onward)	Flagged Intervention Paracentesis Flag, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Parenteral nutrition flag (01/02 – onward)	Flagged Intervention Parenteral Nutrition Flag, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Pleurocentesis flag (01/02 – onward)	Flagged Intervention Pleurocentesis Flag, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Radiotherapy flag (01/02 – onward)	Flagged Intervention Radiotherapy Flag, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Tracheostomy flag (01/02 – onward)	Flagged Intervention Tracheostomy Flag, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> Vascular access device flag (01/02 – onward)	Flagged Intervention Vascular Access Device Flag, based on the CIHI CMG Plus grouping methodology
<input type="checkbox"/> CACS_CODE (Comprehensive Ambulatory Classification System grouping) (06/07 – onward)	CACS Code
<input type="checkbox"/> CACS RIW (06/07 – onward)	Ambulatory weighting value assigned to the case by the CIHI CACS grouper



MEDICAL SERVICES PLAN (MSP) PAYMENT INFORMATION CHECKLIST

Submit this completed form to the email address:
healthdatacentral@gov.bc.ca

Questions about the request process or any part of this application may be directed to
the email address above.

MINISTRY OF HEALTH USE ONLY

File Number

Date Received

PROJECT TITLE

APPLIES TO COHORT(S)

DATE RANGE

From (yyyy/mm/dd)

To (yyyy/mm/dd)

OTHER DATE RANGE CRITERIA

MEDICAL SERVICES PLAN PAYMENT INFORMATION (January 1, 1990 onwards)

The data includes MSP insured medical fee-for-service and alternate payment services provided by general practitioners and specialists. It also includes MSP insured services provided by other health practitioners such as chiropractors, naturopaths, physical therapy, oral surgeons, podiatrists, optometrists, dental surgeons, oral medicine, orthodontists, massage practitioners, acupuncturists and midwives.

These data do NOT include therapeutic abortion data in accordance with the *BC Freedom of Information and Protection of Privacy Act*.

DATA VARIABLES	DEFINITION
<input type="checkbox"/> Personal Identification Number Replaced by project-specific Patient Study Identification number	Identification number of person receiving the health care service.
<input type="checkbox"/> Client Gender	Client gender is the sex of the client.
<input type="checkbox"/> Client Age Group	Client Age Group is the 5 year cohort that clients are grouped into based on their age at time of service.
<input type="checkbox"/> Client HA	The Client Health Authority is a one-digit code that identifies the HA within BC in which the patient lives.
<input type="checkbox"/> Client HSDA	The Client Health Service Delivery Area is a two-digit code that identifies the HSDA within BC in which the patient lives.
<input type="checkbox"/> Client LHA	The Client Local Health Area is a three-digit code that identifies the LHA within BC in which the patient lives. (Please provide rationale when requesting this variable).
<input type="checkbox"/> Client FSA	Forward Sortation Area.

DATA VARIABLES	DEFINITION
<input type="checkbox"/> Other Client Geographical Information	Other geographical divisions from Statistics Canada (i.e. CMA, CSD, CD) could be requested, as well as researcher defined geographical units.
<input type="checkbox"/> Service date	Service date is the date on which the service was rendered by a practitioner.
<input type="checkbox"/> Fee Item	Fee Item Code is a numeric code used to identify each service provided by a practitioner.
<input type="checkbox"/> Service code	Service Code is a two-digit code to indicate the type of services rendered by a practitioner.
<input type="checkbox"/> ICD9 diagnostic code	Diagnostic codes are intended to indicate the condition for which the patient is treated. The MSP diagnosis codes are based on ICD9 (9TH version of the International Classification of Disease) for diagnostic coding.
<input type="checkbox"/> Paid service	This is the number of services paid by MSP to the practitioner in the fee-for-service claim.
<input type="checkbox"/> Expenditure	Expenditure in the fee-for-service claim describes the paid amount from a Medical Services Plan expenditure perspective.
<input type="checkbox"/> Encounter Claim service	This is the number of services submitted by practitioner in the encounter claim. These services are paid under an alternative payment (non fee-for-service) basis.
<input type="checkbox"/> Payee number Replaced by project-specific identification number	Payee number is the practitioner, hospital, office, institution, etc. to which the payment of a claim is made.
<input type="checkbox"/> Claim type	Claim type is a two-character variable which identifies the type of practitioner and the responsibility (insurer) for paying the claim.
<input type="checkbox"/> Practitioner number Replaced by project-specific identification number	Practitioner Number is a number, assigned to a practitioner, which is used on a claim to identify the practitioner who rendered the service to an insured person.
<input type="checkbox"/> Claim specialty	The Claim Specialty is the specialty recorded on the claim by the Edit and Eligibility sub-system of MSP Claims. It represents a practitioner's specialty associated with a claim assigned at the time when the claim was processed.
<input type="checkbox"/> Referring practitioner number Replaced by project-specific identification number	The Referring Practitioner Number for a Claim is the MSP practitioner number of the practitioner who referred the service, usually a physician.
<input type="checkbox"/> Client Province	Client province is a two-character variable which is intended to indicate where the client is resident.
<input type="checkbox"/> Service place	Service place is the geographical place where the service was provided.
<input type="checkbox"/> Service location	Service Location is used to indicate what type of facility a procedure was performed in.



PHARMANET DATA CHECKLIST

Submit this completed form to the email address:
healthdatacentral@gov.bc.ca

Questions about the request process or any part of this application may be directed to the email address above.

MINISTRY OF HEALTH USE ONLY

File Number

Date Received

PROJECT TITLE

APPLIES TO SUBPOPULATIONS

DATE RANGE

From (yyyy/mm/dd)

To (yyyy/mm/dd)

OTHER DATE RANGE CRITERIA

PHARMANET FILES (January 1, 1996 to present)

PharmaNet data includes records of all medications dispensed in community pharmacies in BC. PharmaNet dispense data is available from two files; medication history and claims history. Medication history contains records for all dispenses in BC regardless who pays for the claim. Claims history contains claim records for all dispenses except those for individuals who are known to be federally insured (Veterans, RCMP, Armed Forces and beneficiaries of Non-Insured Health Benefits).

PharmaNet does not capture:

- Medications administered to hospital in-patients
- Antiretroviral medications dispensed from the Centre of Excellence in HIV / Aids at St. Paul's Hospital
- Chemotherapy agents dispensed by the BC Cancer Agency
- Medications purchased without a prescription may not be on PharmaNet (e.g., over the counter medications, herbal products, vitamins)
- Medication samples dispensed at a physician's office (some are entered by physicians with PharmaNet access)
- Third party paid amounts
- Medication cost information for federally insured individuals (RCMP, Canadian Forces, Veterans and beneficiaries of Non-Insured Health Benefits Program)

PATIENT INFORMATION

<input type="checkbox"/> PHN Replaced by project-specific patient identification number
<input type="checkbox"/> Gender
<input type="checkbox"/> Date of birth (YYYYMM)
<input type="checkbox"/> Age (calculated as of Jan 1 for each year of data)
<input type="checkbox"/> Patient Health Authority (HA)

☐ Patient Health Services Delivery Area (HSDA)

☐ Patient Local Health Area (LHA)

Research rationale describing why this field is required must be supplied before it will be considered for release:

☐ Forward Sortation Area (FSA)

Research rationale describing why this field is required must be supplied before it will be considered for release:

☐ Other patient geographic information – please describe:

Research rationale describing why this field is required must be supplied before it will be considered for release:

PHARMACY INFORMATION

☐ Pharmacy identification number

Replaced by project-specific practitioner identification number

☐ Pharmacy Health Authority (HA)

☐ Pharmacy Health Services Delivery Area (HSDA)

☐ Pharmacy Local Health Area (LHA)

Research rationale describing why this field is required must be supplied before it will be considered for release:

☐ Other Pharmacy geographic information – Please Describe:

Research rationale describing why this field is required must be supplied before it will be considered for release:

PRACTITIONER INFORMATION

<input type="checkbox"/> Practitioner identification number Replaced by project-specific practitioner identification number
<input type="checkbox"/> Practitioner Health Authority (HA)
<input type="checkbox"/> Practitioner Health Services Delivery Area (HSDA)
<input type="checkbox"/> Practitioner Local Health Area (LHA) <i>Research rationale describing why this field is required must be supplied before it will be considered for release:</i>
<input type="checkbox"/> Other Practitioner geographic information – Please Describe: <i>Research rationale describing why this field is required must be supplied before it will be considered for release:</i>
<input type="checkbox"/> Practitioner identification reference (code identifying the governing body from which practitioner receives licence)
<input type="checkbox"/> Practitioner type (e.g., physician, dentist, nurse practitioner, podiatrist, midwife, veterinarian, pharmacist)
<input type="checkbox"/> Practitioner specialty flag Y/N
<input type="checkbox"/> Practitioner specialty type description (e.g., cardiology, neurology, paediatrics, urology)

RECORDS REQUESTED FOR (Choose one of the following)

<input type="checkbox"/> All medications
<input type="checkbox"/> Medications for drugs listed in drug file provided by applicant
<input type="checkbox"/> Multiple drug lists provided. Please describe drug list use by cohort (i.e. use drug list 1 for cohort 1):

DRUG INFORMATION

<input type="checkbox"/> DINPIN (drug information number as per drug list provided, field is mandatory)
<input type="checkbox"/> Canadian brand name
<input type="checkbox"/> Chemical/generic name
<input type="checkbox"/> GCN sequence number (random number representing generic formulation of drug assigned by Health Canada)

<input type="checkbox"/> Drug strength
<input type="checkbox"/> Drug form units (e.g., ml, grams, each)
<input type="checkbox"/> Dosage form code and description (e.g., aerosol, tablet, capsule, liquid)
<input type="checkbox"/> AHFS code (American Hospital Formulary code assigned and maintained by Health Canada)
<input type="checkbox"/> PharmaCare Theraclass (PharmaCare therapeutic class assigned and maintained by PharmaCare)

MEDICATION REVIEW

<input type="checkbox"/> Medication Review Records (as of April 1, 2011) NOTE: claims record field values: PIN = 99000501 or 99000502 or 99000503, drug cost = 0, quantity and days supply = 1 and prescriber type = pharmacist. (Standard 99000501, Pharmacist Consultation 99000502 and Follow-up = 99000503)

MEDICATION/DISPENSING INFORMATION

<input type="checkbox"/> Date of service (date dispensed)
<input type="checkbox"/> Quantity dispensed
<input type="checkbox"/> Days supply (estimate of number of days of prescription treatment)

CLAIMS INFORMATION

<input type="checkbox"/> Date of service (date dispensed)
<input type="checkbox"/> Account code and description (Account type under which claim adjudicated)
<input type="checkbox"/> Quantity (actual quantity dispensed)
<input type="checkbox"/> Quantity accepted (pro-rated based on days supply accepted for payment by PharmaCare)
<input type="checkbox"/> Days supply (estimate number of days of treatment as submitted by pharmacist)
<input type="checkbox"/> Days supply accepted (submitted amount may be reduced if greater than Special Authority, plan or DINPIN amount)
<input type="checkbox"/> Drug cost claimed by pharmacist
<input type="checkbox"/> Drug cost accepted by pharmacist
<input type="checkbox"/> Drug cost paid (submitted drug cost amount paid by PharmaCare)
<input type="checkbox"/> Professional fee (dispensing fee claimed by pharmacist)
<input type="checkbox"/> Professional fee accepted (dispensing fee amount accepted by PharmaCare)
<input type="checkbox"/> Professional fee paid (dispensing fee amount paid by PharmaCare)
<input type="checkbox"/> Special services fee (total amount claimed by pharmacist for special service e.g., consulted prescriber, action Rx issue)

SECURE FILE TRANSFER PROTOCOL (SFTP) PROCESS DOCUMENT

OVERVIEW

The **Secure File Transfer Service (“SFTP”)** is a service providing the means to securely transfer electronic files between authorized users. **SFTP** or Secure File Transfer Protocol is a secure file transfer tool between a SFTP server and user, using a SFTP client or SFTP software. The file is encrypted during the transfer, but not while it is sitting on the server. All clients must have SFTP software installed before the SFTP mail boxes are setup.

DATA EXCHANGE

Personally Identifiable Data refers to information that would allow the identification of an individual by direct means, such as a PHN or SIN, or by a combination of information that would allow the deduction of the identity of an individual, such as gender, birth date and postal code.

Information Sharing Agreement (ISA) is a generic term referring to a document that describes and authorizes the sharing of data between two parties.

Information Sharing Plan (ISP) refers to the document that describe the framework for data access or data exchange between the Ministry and the Applicant (e.g. Health Authorities etc...) and the conditions of their access.

Health Authority Schedule 15 to Overarching Agreement – Refers to the document that describes the data exchange between the Ministry and the Health Authorities. The Information Sharing Plan is replacing the Schedule 15 under the General Information Health?

Summary of the Application Process

To initiate the process to set up SFTP, the analyst responsible for a project in IMKS fills out the Secure File Transfer request form located at:

s.15

➤ **Please note:** When attaching the ISP/ISA or Schedule 15's to the form it must be the final signed copy in order to the SFTP request to be processed.

➤ All secure file transfer requests for projects must be approved by the A/Director (Melissa Murdock) of IMKS.

➤ The A/Director approves it and forwards the form and the approval to the Health Data Access Services (HDAS) <mailto:Hlth.HnetConnection@gov.bc.ca>

➤ Please be aware that this is only transitory storage space. Files will be automatically deleted after 30 days.

➤ **Please Note:** Processing time for the SFTP request by the Connections Group will take anywhere between 40 to 60 business days at this time.

Adding additional individuals for access to data

If additional individuals are being added, or removed at a later date to the SFTP form for data access the analyst prepares an email that includes the SFTP request #, project #, and title as well as the names that are being added or removed and forwards the request to the original approver (**Director approving SFTP form**). Once the Director has approved the email is then forwarded to:
<mailto:Hlth.HnetConnection@gov.bc.ca>

➤ **You must complete all mandatory fields * in order for the form to be processed.**

Ministry Business Area Title:

*Branch

Information Management and Knowledge Servs

Ministry Business Area User

(*The names below are currently the staff that will be responsible for the data linkage and transfer to requester)

*Name

Gay Corbett/ Muhammad Anwer/Paul Young

*Telephone

(xxx-xxx-

xxxx)

*Email
Address

@gov.bc.ca

External User Information

Note: if you are planning an unattended, automated transfer, please provide your IT contact in addition to end user contacts.

***Name of External User: This is the person who is going to be receiving and access the data. This will not be the IT contact for organization**

e.g. Ronald MacDonald

*Organization

Cancer Agency

*Street Address/PO Box

200 Terminal Street

*City

Vancouver

*Province

BC

*Postal Code

V8C 9N5

*Telephone (xxx-xxx-xxxx)

*Email Address

SFTP IT Contact Information

This information should be provided to the IMKS analyst responsible for the project by the client (HA, org. etc.) requesting the data.

IMPORTANT! This person identified must be able to assist in the gathering of network information (i.e. IP address) and coordinate software installations.

*Name of IT Contact

Joe IT

*Job Role

IT Service Consultant

*Telephone (xxx-xxx-xxxx)

*Email Address

IMPORTANT: Please ensure IT Contact is correct otherwise it will delay the implementation of the request.

*Description of the data being transferred. Give a brief description of the type of data being requested

Please include the filename of the ISP/ISA or Schedule e.g. 13-019 Population-based Physician Resource Planning - VIHA has requested de-identified MSP records.

Are you transferring personally identifiable data? ☐ Yes ☐ No

Currently, the response has to be Yes otherwise it will not allow you attach the file if the response is no. The form is in the process of being changed so that the file can be attached if it is not identifiable data.

*In order to determine which service best fits your needs please provide a description of how you wish to transfer your data. For example, will you be transferring from your PC to another PC, or from your PC to a server or needing an automated transfer from one server to another?

For most of the HA projects the response should be PC to another PC. There may on occasion times where automated transfers are requested

a. How often will you be transferring files?

One Time Only

The selection box gives you the option to choose the number of times e.g. daily, weekly, monthly, quarterly, or other

Note: If this is a one time only transfer, the mailbox will be deleted after 30 days.

*b. Is any file larger than 70 MB? ☐ Yes ☒ No

The majority of the time the file will not be larger than 70 MB

*c. How many files? Put the number of files being transferred – for the majority of the time it will only be one

*d. What is your preferred username?

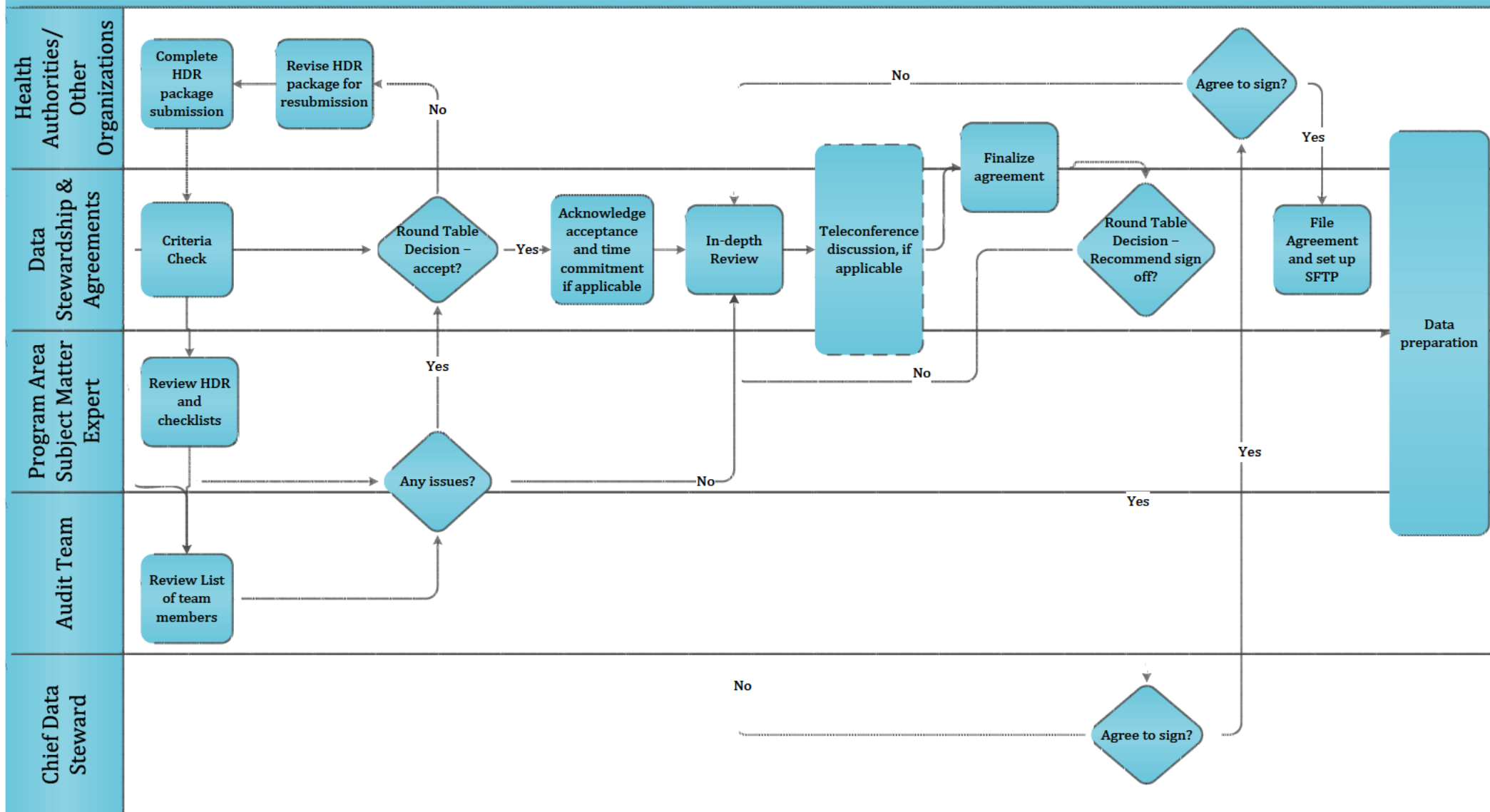
Number and title of the project: e.g. 13-019 Population-based Physician Resource Planning

Email address of Approver *(To be approved by the Director of the Program Area making this request.)* **for IMKS it will be Melissa Murdock**

Check here to have a copy CC'd to you ☒

DRAFT

Health Authorities/Other Organizations – Health Data Request form/ISP/ISA



GHISA GUIDE



**Detailed User Guide to the
General Health Information Sharing Agreement
November 2012**

TABLE OF CONTENTS

1.	What is the GHISA?.....	3
2.	What does the GHISA apply to?	3
3.	Does the GHISA commit the parties to share any particular information? .	3
4.	Does the GHISA do away with all other legal documentation for health information sharing?	4
5.	Does the GHISA do away the need for Privacy Impact Assessments?	4
6.	How does the GHISA relate to existing agreements?	4
7.	Who oversees the administration of the GHISA? How are disputes resolved?	4
8.	How does the GHISA govern physicians?	5
9.	How does the GHISA apply to information systems used to share health information amongst the parties?	5
10.	What is the Common Access Management Framework?.....	7
11.	What if the access model for existing systems is significantly different than the approaches recommended by the Common Access Management Framework?	7
12.	What is a Terms of Management for a GHISA System?.....	8
13.	What does the GHISA say about Information Management and Information Security Policies?	8
14.	Does the GHISA cover sharing of information with Providence Health Care (PHC) and other service providers/affiliated organizations?.....	9
15.	Does the GHISA cover sharing of information with private healthcare providers such as physicians in private practice?.....	10
	Attachment: GHISA Documentation Requirements Chart.....	11

Guide Purpose:

The purpose of this guide is to help those involved in projects, programs and other activities which require the sharing of health and health-related information amongst the health authorities and/or the Ministry of Health, to understand how the General Health Information Sharing Agreement (GHISA) applies and supports such activities.

1. What is the GHISA?

- a. The GHISA is intended to establish a common legal, policy and governance framework for the sharing of health information and ancillary personal information within the public healthcare system going forward. The parties to the agreement are Ministry of Health and the 6 health authorities. **[Recital H, GHISA]**
- b. The GHISA does not independently authorize the sharing of any particular information, but rather documents the fact that such authorization exists in FIPPA or in other legislation and sets out the rights and obligations of the parties when information is shared.

2. What does the GHISA apply to?

- a. It applies to all sharing of health information and health-related information, including health service delivery information, amongst the Ministry of Health and/or the health authorities for provision of care purposes and secondary purposes on a go forward basis, except health information in Health Information Banks that is subject to the *eHealth (Personal Health Information Access and Protection of Privacy) Act* (the "eHealth Act"). **[see definition of "Data"; ss. 2.2 to 2.5 GHISA]**
- b. It does not apply to the sharing of employee information or other health provider information, except to the extent such information is required in relation to managing employees or health providers as it relates to their access to and use of health information shared under the GHISA. **[see definition of "Data" GHISA]**

3. Does the GHISA commit the parties to share any particular information?

- a. No, the GHISA only documents the parties' intentions to share information with each other that is reasonable, relevant and necessary for delivering healthcare services or in relation to healthcare planning and other secondary uses of health information. It does not identify any particular information that must be shared. Furthermore, all information sharing must be permitted under FIPPA and other laws. Each party retains its discretion as to whether to share any particular information, including where it believes it has no authority to disclose or is prohibited from disclosing under FIPPA or a contractual obligation. **[s. 2.1, s. 4.1 GHISA]**

4. Does the GHISA do away with all other legal documentation for health information sharing?

- a. No. Please see the **GHISA Documentation Requirements Chart** attached to this Guide for more details and examples of when additional documentation is required.

5. Does the GHISA do away the need for Privacy Impact Assessments?

- a. No, privacy impact assessments (PIAs) are still required in order for the parties to meet their obligations under s. 30 and other provisions of FIPPA. Any questions about whether a PIA is required for a project, program, system or other information sharing activity should be referred to the appropriate Ministry of Health or health authority Information Privacy Office. **[s. 3.6 GHISA]**
- b. The GHISA sets out certain principles and approaches for PIAs that are done in respect of information sharing situations amongst the parties. **[s. 3.6 GHISA]**

6. How does the GHISA relate to existing agreements?

- a. Existing agreements will continue in force unless expired or terminated by agreement of the parties and/or replaced by way of additional documentation contemplated under the GHISA. **[s. 2.4 GHISA]**

7. Who oversees the administration of the GHISA? How are disputes resolved?

- a. The GHISA creates a new committee called the GHISA Steering Committee, a subcommittee of the Health CIO Council, consisting of one senior representative from each party, to act as the overall

stewardship and decision-making body with respect to key issues arising under the GHISA. **[s. 7.1 GHISA]**

- b. Despite the GHISA Steering Committee's role in decision-making, each party retains the right to choose whether to share information within its control with any of the other parties. See Question 3. **[s. 7.1(c), s. 4.1 GHISA]**
- c. Issues that cannot be resolved by the GHISA Steering Committee/Health CIO Council are referred to the CEOs of the health authorities and the Deputy Minister of Health (Leadership Council). **[s. 7.3 GHISA]**

8. How does the GHISA govern physicians?

- a. Physicians who are employed by or privileged to practice within a health authority's facility and who deliver services on behalf of a health authority are governed by the GHISA as though they are staff of the health authority. **(see definition of "Personnel")**
- b. Physicians acting in a capacity that is independent from a health authority, such as in their private practice must sign a separate agreement (which will include applicable terms the GHISA) with the party through which they are accessing information shared under the GHISA. **[s. 6.2 GHISA]**

9. How does the GHISA apply to information systems used to share health information amongst the parties?

- a. The GHISA creates the concept of a "GHISA System" or system that is used to facilitate the sharing of information between the parties under the GHISA. This includes systems in which two or more parties contribute data as well as internal systems of parties which they make available for access by one or more of the other parties. **[s. 5.1 GHISA]** There are two categories of GHISA Systems as described in the chart below: **[s. 5.3 GHISA]**

GHISA System Category	System Definition	Examples	GHISA Terms/Requirements
Category A	A system that is only subject to the general terms and conditions of the GHISA, such as an internal system made externally accessible at the option of the owner	s.15	<ul style="list-style-type: none"> Standard access and security terms and conditions of the GHISA apply, which may be supplemented by additional terms at the discretion of the system/data owner Once developed and adopted by all parties, common IMIS policies** apply automatically; where common policies do not exist, policies of the system owner govern
Category B	A system in which the data is contributed to by two or more parties and is designated by the parties as a Category B GHISA System, such that additional terms apply in addition to the general terms applicable to all GHISA Systems	<u>Potentially suitable for Category B designation:</u> s.15	<ul style="list-style-type: none"> Standard access and security terms and conditions of the GHISA apply Common Access Mgmt Framework, including consistent protocols for release of data for secondary use Terms of Management (approved by all participating parties) Once developed and adopted by all parties, common IMIS policies** apply automatically; where common policies do not exist, policies of the Central Office* govern
<p>*The term "Central Office" refers to the party that is responsible for the administration and operation of the system.</p> <p>**Health Authorities will work towards having a set of common IMIS (Information Management/Information Security) policies that will apply to their respective systems while the Ministry of Health will comply with the BC Government's Information Security Policy in respect of its systems. See Question 13 of details.</p>			

- b. The parties will maintain a register of Category B GHISA Systems. **[s. 5.5(e) GHISA]**
- c. Health Information Banks under the eHealth Act and PharmaNet are excluded as being GHISA Systems. **[s. 5.2 GHISA]**
- d. The party(s) that has custody and/or control of information within a Category B GHISA System will be specified in the Terms of Management for that system. **[s. 5.5(b) GHISA]**
- e. Information within a Category B GHISA System that becomes inextricably integrated into a consolidated set of records will be made available to all parties that contributed to the creation of such records and each party will retain a copy (based on the date in which the party started contributing) in the event that a system ceases to operate or if the GHISA is terminated. **[s. 4.5(b), s. 8.2 GHISA]**

10. What is the Common Access Management Framework?

- a. The Common Access Management Framework will be a set of principles, approaches and rules that lay the foundation for how access to Category B GHISA Systems will be enabled, controlled and managed. **[s. 5.5(a) GHISA]**
- b. The Common Access Management Framework will include a common approach to assigning access privileges to users with the goal of increasing consistency of access privileges across different Category B GHISA Systems. **[s. 5.4(a)(i) GHISA]**
- c. The Framework is intended to bring consistency to privacy controls such as disclosure directives, masking, enhanced information security, clinical relationship attestation and dealing with access to highly sensitive information for Category B GHISA Systems. **[s. 5.4(a)(ii) GHISA]**
- d. The Framework will also establish common approaches for access to and release of information from Category B GHISA Systems for secondary uses, including research. **[s. 5.4(a)(iii) GHISA]**

11. What if the access model for existing systems is significantly different than the approaches recommended by the Common Access Management Framework?

- a. Changes to access models would be expected to occur over time as parties are reasonably able to implement given existing systems and infrastructure. The Common Access Management Framework will be

flexible and high level enough to accommodate various implementations of the agreed upon approaches set out in the Framework. **[s. 5.5(a) GHISA]**

- b. All parties will participate in the development of the Common Access Management Framework and it would be approved by the GHISA Steering Committee to ensure that the Framework is feasible and suitable for all parties. **[s. 5.5(a) GHISA]**
- c. The Common Access Management Framework will only apply to Category B GHISA Systems, which must be specifically designated as such by the GHISA Steering Committee. **[s. 5.3, s. 5.5(a) GHISA]**

12. What is a Terms of Management for a GHISA System?

- a. A Terms of Management is a document that sets out details for how a Category B GHISA System and its data will be managed. There is no prescribed format, but may include topics such as:
 - i. A description of the general purpose(s) of the system;
 - ii. The System Owner(s);
 - iii. The Parties and Healthcare Third Parties that input their Data into or make their Data available via the system;
 - iv. The Parties and Healthcare Third Parties that have access to the system;
 - v. The designated Central Office for the system;
 - vi. The Party(s) that has custody or control of the Data contained in or made accessible through the system;
 - vii. The data steward or person or group of persons responsible for making decisions with respect to whether Data contained in or made accessible through the system should be provided or made accessible to a particular user, group of users or data requestor;
 - viii. The process for obtaining access privileges into the system or obtaining Data from the system for both provision of care and Secondary Uses;
 - ix. Whether the system is subject to HA IMIS Policies or MOH IMIS Policies or equivalent policies of the Central Office; and
 - x. Other information deemed appropriate or required by the participating Parties. **[s. 5.5(b) GHISA]**

13. What does the GHISA say about Information Management and Information Security Policies?

- a. The parties agree to work to establish common Information Management/Information Security (IMIS) policies. Having common

IMIS policies is essential to creating a trusted network amongst the parties for information sharing. It is important for each disclosing party to know that when it shares information with another party such information will be protected by the application of similar or the same policies for information management and security in the hands of the receiving party. **[s. 3.7 GHISA]**

- b. The common IMIS policies will be developed at a level of granularity that is sufficient to require specific protocols and approaches to information management and protection, but not so prescriptive and specific that the parties will not be able to comply or reasonably work toward compliance with the policies across the various systems and processes that they currently employ.
- c. The GHISA distinguishes between health authority (HA) common IMIS policies and Ministry of Health (MOH) IMIS policies in recognition of the fact that MOH is subject to BC government information security policies which it cannot alter. The HA common IMIS policies will apply to GHISA Systems that are controlled by the HAs and information in the possession of the HAs and the MOH IMIS policies will govern systems controlled by MOH and how information is treated while in the possession of MOH. The health authorities will work towards making the HA common IMIS policies substantially similar to the MOH IMIS policies. **[s. 3.7 GHISA]**
- d. The Terms of Management for Category B GHISA Systems may specify which policies apply so that staff are clear about the rules that they must follow. **[s. 3.7(c), s. 5.5(b)(ix) GHISA]**

14. Does the GHISA cover sharing of information with Providence Health Care (PHC) and other service providers/affiliated organizations?

- a. Yes, but additional documentation is required. Organizations which are affiliated with or service providers of health authorities will be required to sign a separate agreement that makes them subject to the applicable terms of the GHISA should they receive or be provided with access to health information shared under the GHISA. It will be the responsibility of each party to the GHISA to enter into such agreements with these third parties who may be given access to health information, although the parties may collaborate to develop agreement templates in this regard. **[s. 6.1 GHISA]**
- b. Each party will be accountable to the other parties for the actions of affiliated organizations, service providers or other third parties to

whom it discloses information shared under the GHISA. **[s. 6.1 GHISA]**

15. Does the GHISA cover sharing of information with private healthcare providers such as physicians in private practice?

- a. The GHISA contemplates that the parties will share health information with healthcare providers outside of health authorities and who are also not necessarily affiliated with a health authority. Similar to health authority affiliated providers, such “private healthcare providers” will be required to sign a separate agreement that makes them subject to the applicable terms of the GHISA should they receive or be provided with access to health information shared under the GHISA. It will be the responsibility of each party to the GHISA to enter into such agreements with these third parties who may be given access to health information, although the parties may collaborate to develop agreement templates in this regard. For example, the parties would likely develop a template Data Access Agreement for physicians in private practice who wish to have access to a GHISA System. **[s. 6.2 GHISA]**

[Attach GHISA Documentation Chart]

DRAFT

Health Authority (HA)**Continuous Improvement – Deliverables**

	Enhancements	Action
1.	DARTS database – update, streamline & standardize	COMPLETE – April 2013
2.	Prepublication Review Submission process - streamline & standardize	COMPLETE – July 2013
3.	Health Data Central Website – develop and implement	COMPLETE – May 2013
4.	Health Data Requests form, checklists, linkage strategy and process - streamline & standardize	COMPLETE – August 2013
5.	General Health Information Sharing Agreement (GHISA): Information Sharing Plan (ISP) Template - develop	COMPLETE – May 2013
6.		
7.		

Monthly Ethics Report

July 2013 expiries:

Project Name	Project Number	Ethics Certificate Number	Ethics Expiry Date	Results
Tyndall	04-011	H02-50263	22-Jul-2013	Ethics renewal to June 18, 2014
Dahlgren	04-018	H03-70343	8-Jul-2013	Ethics renewal to June 10, 2014
Davies-Koehoorn	05-003	H04-80270	30-Jul-2013	Ethics renewal to July 16, 2014
McBride	05-036	H05-60113	10-Jul-2013	Ethics renewal to June 26, 2014
McBride	09-015	H09-01957	10-Jul-2013	Ethics renewal to July 9, 2014
Khan	09-016	H08-02579	8-Jul-2013	Ethics renewal to June 26, 2014
Wong	10-014	H10-01417	5-Jul-2013	Email sent to MOH indicating closure in process July 4, 2013.
McGrail	10-015	H10-02693	5-Jul-2013	Ethics renewal to May 17, 2014
Wong	11-001	H10-02355	18-Jul-2013	Ethics renewal to June 26, 2014
Palepu	11-014	U of Ottawa 04-08-09	9-Jul-2013	Outstanding (MOH notified July 8, 2013)
Dahlgren	12-009	CW10-0176/ H10-00336	17-Jul-2013	Ethics renewal to July 8, 2014

Outstanding from previous months:

Project Name	Project Number	Ethics Certificate Number	Ethics Expiry Date	Status
Stothers	11-006	H03-70638	9-Nov-2012	Res. has not yet received data; data will not be released without ethics renewal.

New Health Data Request Form - Health Authority– Detailed

The ministry has a General Health Information Sharing Agreement (GHISA) with health authorities to provide a framework for information management.

An Information Sharing Plan (ISP), as a Schedule to the GHISA, between the ministry and health authorities outlines the terms and conditions under which record-level data is exchanged between the ministry and the health authorities for the purposes of program planning and evaluation, surveillance activities, and "Healthcare Delivery & Related Purpose" as defined under GHISA. Please complete and submit the [Health Data Request form](#) ^(PDF 613K) to initiate the development of the agreement.

The Process

1. Submission to the Ministry

Requestor completes the [Health Data Request form](#) ^(PDF 613K) (HDR) and submits to the ministry with all supporting documentations.

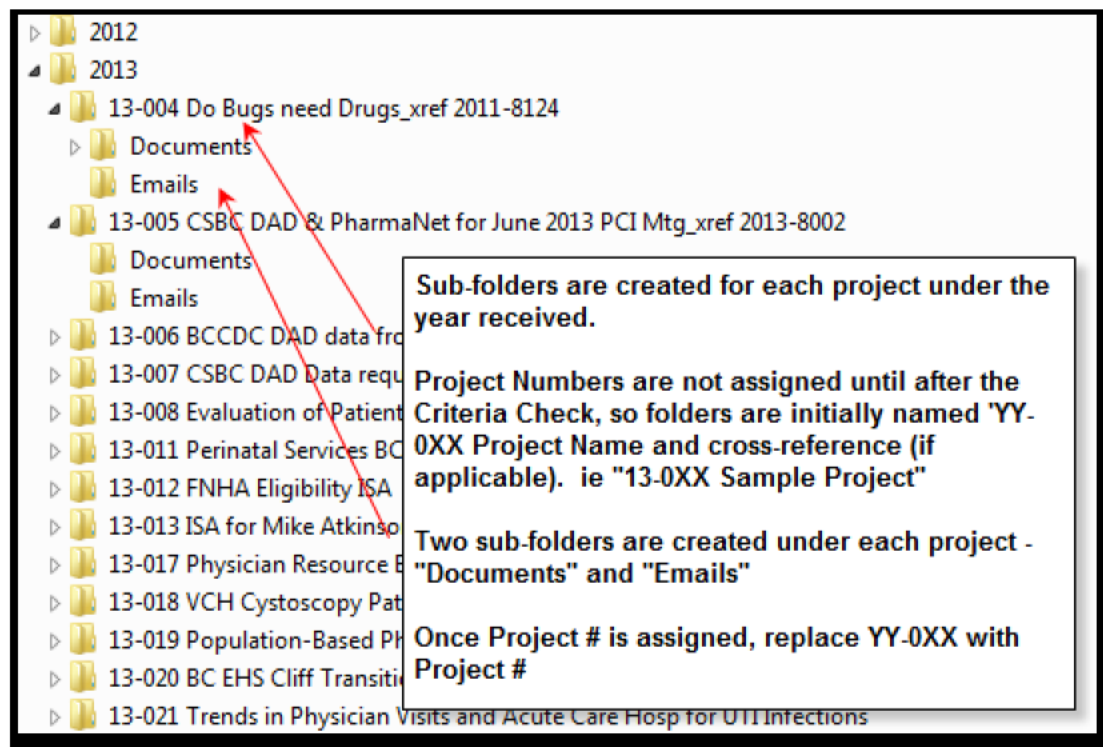
The Inbox Administrator forwards the new HDR package to the appropriate Analyst.

- Cornel Lencar if the HDR has a PharmaNet (PNet) component
- Lina Bennett if there is no PNet component

The Inbox Administrator creates a folder for the HDR project and saves the email and supporting documentation to the LAN

s. 15

See below folder structure creation format:










Inbox Administrator saves the original email in the EMAIL folder and each supporting document in the DOCUMENTS folder. All emails and documentation are to be saved with the following format:












YYYY-MM-DD – 'meaningful description of email/doc' – PROJECT_TITLE – Project# (if available)

See examples below:

EMAILS

	2013-01-10 BCCDC further amendment request.msg	2
	2013-01-10_from BCCDC_DBND Proposed Amendments to Sched. 15 agreement.msg	2
	2013-01-29 response from Catherine RE 2011-8124 DBND - Proposed Schedule Amen...	2
	2013-02-14 DBND- new data access request.msg	2
	2013-02-14 from Karen to Ciaran FW Do Bugs Need Drugs - new data access request.m...	2
	2013-02-19 from Catherine to Rosemary re 2013-004 Follow-up Timelines for DBND D...	2
	2013-02-19_Timelines for DBND Data Extract.msg	2

DOCUMENTS

	2013-004_Schedule 15_Do_Bugs_Need_Drugs_v.3Clean.doc
	2013-004_Schedule 15_Do_Bugs_Need_Drugs_v.3Track Changes.doc
	Response to subject matter experts_Mar11.13.docx
	HA_Administrative Update Template_Do_Bugs_Need_Drugs_DRAFT_Feb12.13....
	NEW_2013-004_Schedule 15_Do_Bugs_Need_Drugs.doc
	NOTE TO FILE.docx
	2011-8124_Schedule 15_Do_Bugs_Need_Drugs_Amended_DRAFT_Feb12.13.doc
	PSD_Contract #2009-DBND - Schedule A.pdf
	2011-8124_Schedule 15_Do_Bugs_Need_Drugs_Amended_DRAFT_Jan9.13.doc
	HA_Administrative Update Template_Do_Bugs_Need_Drugs_DRAFT_Jan9.13.d...
	DBND Administraive Data Issues.docx

Inbox Administrator records New/Pending HDR on Criteria Check Queue Whiteboard:

**** Criteria Check Queue Whiteboard is located across from Karen Li's cubicle (between Pillar C0 and C1) ****

The Analyst conducts the Criteria Check on the HDR application. The Criteria Check must be completed **within 1 month** of receipt of the HRD..

The Analyst reviews on the following:

Completeness and Consistency:

- Check that Project Title, Team Members and Roles, and all project details are consistent between all documentation – HDR, Checklists, External Variables, etc.
- If there is a difference in Project Titles between documentation, ensure justification is provided
- Check that the data dates requested in the HDR are consistent with those in the Checklists
- Check that the Cohort definitions and dates requested on the Checklists are consistent with the HDR
- Request IT Contact information for SFTP setup

Appropriateness:

- Check that the methodology is clear, while providing an appropriate level of detail
- Check that sound rationale is provided for each database being requested
- Evaluate methodology and the data requested, while respecting the 'Need to Know' principle
- Review Checklists for sensitive data variables being request. If so, ensure strong rationale is provided
- Review accuracy of the Linkage Strategy

Often through the Criteria Check process, questions arise or clarifications are required. **The Analyst** will make note of these and bring them to the Weekly Team Round Table Meeting (**Round Table**). Representatives from the Privacy and Security Branch will attend these meetings for advice on requirements for Privacy Impact Assessments (PIA) and Security Threat Risk Assessments (STRA).

The Analyst determines the Process Category based on the information in the HDR and the Ministry guidelines.

The Analyst briefs the team on the file and all initial questions during **Round Table**. Other members of the team have an opportunity to ask questions about the project. If these questions are deemed valid and appropriate, **The Analyst** adds them to the list of questions for the requestor.

The Analyst emails the Criteria Check confirmation to the Requestor. This email is to include the new Project # (obtained through the DARTS database), Process Category and time commitment (if applicable) and all questions/clarification that arose through the Criteria Check.

See below for a sample template:

Good Morning/Afternoon

Thank you for submitting the Health Data Request and supporting documentation for the project titled, "XXX", received by the Ministry of Health on XXX.

This project reference number is XX-XXX and this is a Category X.

Below is a list of our initial questions:

Thank you,


The Analyst then enters the project into the DARTS database as following:

DARTS - Data Access Request Tracking System

<input type="checkbox"/> Data Entry Form	<input type="checkbox"/> Performance Measurement Report
<input type="checkbox"/> DAR Summary Report	<input type="checkbox"/> Add/Edit Researchers
<input type="checkbox"/> Data File/Source Report	<input type="checkbox"/> Steward List
<input type="checkbox"/> DAR Status Report	<input type="checkbox"/> Database List
<input type="checkbox"/> DARS Audit Report	<input type="checkbox"/> Add/Edit Status
<input type="checkbox"/> Proposal History Report	<input type="checkbox"/> Add/Edit Dropdown Lists
<input type="checkbox"/> Research Web Export	<input type="checkbox"/> Add/Edit Process Category
<input type="checkbox"/> Amendments Status Report	<input type="checkbox"/> Add/Edit Attachment/Doc Type
<input type="checkbox"/> DARS Status Report	<input type="checkbox"/> Add/Edit Publication Type
<input type="checkbox"/> Search	<input type="checkbox"/> Check PrePub Review Due

Click 'Data Entry Form' to create/view Projects

V. 3.8 April 16, 2013

 Notes

DARTS - Data Entry

Go to Request:
New
Name: Saadatsafavi, Mohsen
Select type of request/project (ok to select more than 1)
Close

Request No.: **13-035**

Title: *Continuity, Regularity, and Specialty in COPD Care: An Exploration of Long-term Costs and Health Outcomes*

ISA: ☐ HA: ☐ DAR: ☒ PNET: ☐

DAS: ☐ RTC: ☐ MOU: ☐ Other: ☐

Date Initiated: 04-Jul-13

Popdata No.:

PNet/CeRTS No.:

Project Team Project Details Security Cohorts Project Cycle Notes Status History Amendment Post Agreement Attachment

Principal Investigator/Requestor: Saadatsafavi, Mohsen Access: ☒ Pledge Signed: ☐

Co-Investigators

Co-Investigators	Access	Pledge Signed	
Lynd, Larry	<input checked="" type="checkbox"/>	<input type="checkbox"/>	?
FitzGerald, Mark	<input type="checkbox"/>	<input type="checkbox"/>	?
Marra, Carlo	<input checked="" type="checkbox"/>	<input type="checkbox"/>	?
Stirling, Bryan	<input type="checkbox"/>	<input type="checkbox"/>	?
Sin, Don	<input type="checkbox"/>	<input type="checkbox"/>	?
McGrail, Kim	<input type="checkbox"/>	<input type="checkbox"/>	?
*	<input type="checkbox"/>	<input type="checkbox"/>	?

Indicate if individual requires access to data

Team Members

Team Members	Access	Pledge Signed	
Galo, Jessica	<input type="checkbox"/>	<input type="checkbox"/>	?
Grubisic, Maja	<input checked="" type="checkbox"/>	<input type="checkbox"/>	?
Zafari, Zafar	<input checked="" type="checkbox"/>	<input type="checkbox"/>	?
Raymakers, Adam	<input checked="" type="checkbox"/>	<input type="checkbox"/>	?
Chen, Wenjie	<input type="checkbox"/>	<input type="checkbox"/>	?
*	<input type="checkbox"/>	<input type="checkbox"/>	?

Use dropdown menu to select from existing individuals. If not in list Double Click on Principal Investigator box to enter new member

DARTS - Data Entry

Go to Request:
New
Name: Saadatsafavi, Mohsen
Current Status: Questions to PopData
Close

Request No.: **13-035**

Title: *Continuity, Regularity, and Specialty in COPD Care: An Exploration of Long-term Costs and Health Outcomes*

ISA: ☐ HA: ☐ DAR: ☒ PNET: ☐

DAS: ☐ RTC: ☐ MOU: ☐ Other: ☐

Date Initiated: 04-Jul-13

Popdata No.:

PNet/CeRTS No.:

Project Team Project Details Security Cohorts Project Cycle Notes Status History Amendment Post Agreement Attachment

Peer Review: CV Attached: ☐ Linkage - Y/N: ☐

Funding Source: N/A **Funding Expiry Date:**

Ethics Review: Copy Attached **Version #:** H13-00684 **Ethics Expiry Date:** 03-Apr-14

Process Category: D **3 mth Start Date:** **End Date:**

Resource Allocation: Cornel Lencar **PIA Required:** ☐ **PIA Completed:** ☐ **STR:** ☐

Data Steward Approvals

Please select a database for review: 6 Databases have been selected.

Database / Steward	Date Range	Date Sent	Status	
Continuing Care / Deb McGinnis	1996/01/01-2012/12/31	24-Jun-13	Pending	09-Jul-13
Hospital Separations (DAD) / Deb McGinnis	1996/01/01-2012/12/31	24-Jun-13	Pending	09-Jul-13
MSP Payment Information Master / Deb McGinnis	1996/01/01-2012/12/31	24-Jun-13	Pending	09-Jul-13
MSP Registration and Premium Billing (RP&B) / Deb McGinnis	1996/01/01-2012/12/31	24-Jun-13	Pending	09-Jul-13
PharmaNet / Bruce Carleton	1996/01/01-2012/12/31	24-Jun-13	Pending	09-Jul-13
Vital Statistics Deaths / Jack Shewchuk	1996/01/01-2012/12/31	24-Jun-13	Pending	09-Jul-13

DARTS - Data Entry

[Close](#)

Go to Request: [Dropdown] [Icon]

Request No.: **13-035**

Name: **Saadatsafavi, Mohsen**

Current Status: **Questions to PopData**

Date Initiated: **04-Jul-13**

Popdata No.:

PNet/CeRTS No.:

Title: *Continuity, Regularity, and Specialty in COPD Care: An Exploration of Long-term Costs and Health Outcomes*

Project Team | Project Details | Security | Cohorts | Project Cycle Notes | Status History | Amendment | Post Agreement | Attachment

Individuals to be Contacted: [Dropdown]

Format of Birth/Death Date: Y/M Only

Linkages to Other Data: No

Personally Identifiable Info: [Dropdown]

Data Transfer: [Dropdown]

GeoCode: [Dropdown]

Data Storage/Access
 Office: ☐ PC: ☐
 SRE: ☐ Server/MF: ☐

Location of Notes, Etc.:

Personally Identifiable Info Details/Comments:

DARTS - Data Entry

[Close](#)

Go to Request: [Dropdown] [Icon]

Request No.: **13-035**

Name: **Saadatsafavi, Mohsen**

Current Status: **Questions to PopData**

Date Initiated: **04-Jul-13**

Popdata No.:

PNet/CeRTS No.:

Title: *Continuity, Regularity, and Specialty in COPD Care: An Exploration of Long-term Costs and Health Outcomes*

Project Team | Project Details | Security | Cohorts | Project Cycle Notes | Status History | Amendment | Post Agreement | Attachment

Cohort Type	Cohort Description	Defined By
▶ Cohort 1	All those meeting COPD def (see DAR) between 1/1/96-12/31/12	DAD & MSP
Control 1	2 matched controls for every 1 in cohort -match on Yr of birth, Sex, HSDA an	
*		

Record: 1 of 2 | No Filter | Search

DARTS - Data Entry

Close

Go to Request: ▼ New

Request No.: **13-035**

Title: *Continuity, Regularity, and Specialty in COPD Care: An Exploration of Long-term Costs and Health Outcomes*

Name: **Saadatsafavi, Mohsen**

ISA: ☐ HA: ☐ DAR: ☒ PNET: ☐

DAS: ☐ RTC: ☐ MOU: ☐ Other: ☐

Current Status: **Questions to PopData**

Date Initiated: **04-Jul-13**

Popdata No.:

PNet/CeRTS No.:

Current Status: **Questions to PopData**

Date Initiated: **04-Jul-13**

Popdata No.:

PNet/CeRTS No.:

Project Team
Project Details
Security
Cohorts
Project Cycle Notes
Status History
Amendment
Post Agreement
Attachment

New Status: ▼ Date:

Comments:

Submit

New Status

Cancel

Date	Status	Status Comments
04-Jul-13	Questions to PopData	
04-Jul-13	Request Acknowledged	Request Acknowledged = 'Criteria Check' email sent
24-Jun-13	Request Received	

3. In-depth Review

Ministry staff reviews the application to ensure appropriate use of data according to legislation and policy. Part of the review process may include a teleconference with all stakeholders to discuss the application and clarify questions. Ministry staff develops the ISP to the GHISA to document the terms and conditions.

The Analyst reviews responses from requestor to the initial questions sent out from Criteria Check. If further questions or clarifications are required, the Analyst will schedule a teleconference (T/C) with the requestor and Program Area subject matter experts (SMEs), if appropriate. The Analyst ensures that all issues are discussed to his/her satisfaction during the T/C. The Analyst is responsible for capturing minutes/discussion from the T/C and dissemination to stakeholders. This is intended to be the only round of clarifications/communications.

The Analyst drafts the agreement based on HDR and stakeholder discussions/clarifications. The draft will be reviewed by all stakeholders for finalization.

When the Analyst determines that the in-depth review is complete and ready for decision, he/she prepares the Project Summary and takes the file to Round Table to review responses from questions and T/C discussion. Team Members ensure questions/concerns have been addressed satisfactorily. Project Summary template is located at

s. 15 *Project Summary should not be more than 2 pages.*

4. Agreement Sign-off

The finalized ISP to the GHISA is signed off by both the designated signing authority within the requestor's organization and the ministry's chief data steward. The ministry staff will coordinate this effort.

*The **Analyst** creates a new folder under the "Approvals for Signature" folder*

s. 15

ith the Project # and

Project Title as the folder title.

Save a copy of the Agreement in this folder, along with the:

- *Project Summary*
- *HDR*
- *copies of all Checklists*

*The **Analyst** is to put paper copies of the Project Summary and Agreement in the 'Health Authority Approvals' Folder (black) and notify Karen. Karen will setup time for briefing with CDS if project is complex or sensitive in nature.*

*Once the terms of the agreement have been accepted by CDS, the **Analyst** forwards a pdf copy of the agreement to the requestor for signature. The requestor's signing authority will sign agreement and return to MoH. Once the Agreement has been signed by the CDS, the Agreement is returned to **the Administrator**.*

***Administrator** will:*

- *Scan a copy (pdf) of the Signed Agreement and save it to project folder and Health Authority Agreements in ISA Executed Copies*
- s. 15
- s. 15
- *Provide the original signed hard copy to Janet Harwood for filing*
 - *Email a copy of the Signed Agreement to the requestor*
 - *Update the DARTS db – Status, Data Retention Date*
 - *Save Approval Letter and Summary from "Approvals for Signature" folder to the Project folder (replacing the existing copy)*
 - *Delete all other files from the "Approvals for Signature" (project specific) folder*
 - *Amend Project Updates document to reflect Sign-off complete*
 - *Update tracking spreadsheet*

5. Data Preparation and Delivery

After sign off, the requestor and the ministry begin data preparation according to terms and conditions set out in the ISP to the GHISA. The approved dataset is then transferred securely to the appropriate party via the ministry Secure File Transfer Protocol (SFTP).

*The **Analyst** completes the [Secure File Transfer Request \(7101\) form](#) on behalf of the requestor. When submitted, this form will automatically be sent to the Analyst's Director for approval. The Director must forward the request form with note of their 'Approval' for the SFTP setup to the DAS Connections Group (Connections) at htlh.hnetconnection@gov.bc.ca.*

*Connections has committed to a 5 day turnaround time for processing these requests. Once the SFTP account has been set up, the requestor's users are notified directly by the individual setting up the SFTP and the **Analyst** will be notified of the complete request via email to HealthDataCentral@gov.bc.ca.*

Analyst forwards copy of the signed Agreement to the appropriate program area(s) and Data Linker to advise project is ready to proceed with data preparation. The Analyst will support according to the signed Agreement and Ministry Internal Data Preparation Process (steps outline below).

NOTE:

*The **Analyst** must ensure they 'cc' the DARS Inbox s.15 on **ALL** correspondence, as **the Inbox Administrator** will save all emails in the appropriate LAN location and update the DARTS database accordingly.*

Pre-publication Review Submission Form

PLEASE READ BEFORE SUBMITTING

In signing an Agreement with the Ministry of Health for access to data, the parties agree to send materials to the Ministry of Health in advance of public dissemination. The Ministry of Health is responsible for ensuring appropriate uses of ministry data, that privacy/confidentiality requirements are upheld; there is no gross misuse of the data; and that the data is appropriately referenced.

The Agreement requires that you provide the Ministry of Health, 45 DAYS to review your submission. Materials will be accepted for review only if the COMPLETE form below is provided. Materials that have been previously vetted in a different publication format and do not use new data and/or analysis DO NOT require further vetting.

Please complete the form below for each submission of material intended for public disclosure

Contact name:

Contact email and phone #:

Project number:

Project title:

Type of material for public disclosure:

Please list all Ministry of Health databases relevant to this publication (e.g., MSP, DAD, VSA etc.):

Names of authors:

Names of authors who have access to Ministry of Health data released under this project:

Title of publication:

Please describe how this publication ties to/supports the objectives of this project:

Has this material already been delivered/published?:

If you would like to include additional information (such as details of the journal to which you are submitting or the event at which you are making your material public) please do so here:

Please confirm the following:

I confirm that the attached document is the final draft to be submitted for publication: ☐ Yes

I understand that Ministry of Health requires notification of any pre-publication changes made to this document and a copy of the final publication:

I confirm that this publication does not contain any risk of re-identification of an individual (e.g., small cell sizes, small geographic areas):

I confirm that all relevant Ministry of Health databases are properly referenced (**example of citation to be included in this section**)

Please attach file:

☐ Agreement under which Ministry of Health data was released (e.g. Information Sharing Plan (ISP), Schedule 15 to Overarching Agreement, and Information Sharing Agreement (ISA).

☐ Materials for review

SCHEDULE A

INFORMATION SHARING PLAN TEMPLATE

This Information Sharing Plan (ISP) must be completed in consultation with the Information Privacy Offices of the Parties involved in the Information Sharing Situation this ISP is intended to cover. When completed and approved by each of the participating Parties, this (ISP) forms part of and is subject to the terms and conditions of the General Health Information Sharing Agreement (GHISA). Capitalized terms will have the same meaning as defined in the GHISA.

1. Description of Information Sharing Situation, including the goals or objectives which the information sharing is intended to support:

2. Authorities for Collection, Use and Disclosure under FIPPA and other Applicable Laws:

Section references are to FIPPA unless otherwise specified.

Collection – Authorities for collection for the parties collecting personal information:

☐ **Section 26(a)** – authorized expressly by a law

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 26(c)** – necessary for operating program

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 26(e)** – necessary for planning or evaluating a program or activity of a public body

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 27(1)(a.1)** – indirect collection necessary for medical treatment and it is not possible to collect the information directly from the individual or obtain authority for another method of collection

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 27(1)(b)** – indirect collection from another public body which is disclosing the information under sections 33 to 36

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 27(1)(e)** – necessary for delivering or evaluating a common or integrated program or activity

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Other Applicable Law(s)/section(s):** _____

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

Use – Authorities for use for the parties using personal information:

☐ **Section 32(a)** – use for purpose for which it was collected or compiled

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 32(b)** – use for which the individual has consented

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 32(c)** – use for purpose for which it was disclosed to the public body under ss. 33 to 36

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Other Applicable Law(s)/section(s):** _____

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

Disclosure – Authorities for disclosure for the parties disclosing information:

☐ **Section 33.2(a)** – disclosure for original purpose of collection or consistent purpose

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 33.2(d)** – common or integrated program or activity

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 33.2(l)** – necessary for planning or evaluating a program or activity of a public body

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 33.1(c)** – disclosure authorized or required by an enactment of BC (other than FIPPA) or Canada

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 33.1(1)(e.1)** – disclosure to service provider

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Other Applicable Law(s)/section(s):** _____

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

3. **Specify the categories of information being collected, used and shared, including specifying all or the main data elements where reasonably possible and, in the case of each data element, the reasons why such information needs to be collected, used and shared for purposes of the Information Sharing Situation:**
4. **Specify the categories of individuals within each Party who are authorized to access the information, including whether access to Personal Information is permitted, and the reasons for their access:**
5. **Specify how the information will be shared, with whom(include data flow diagrams) and how it will be secured while in transmission and when in storage, including how access will be controlled:**
6. **Specify the timeline(s) for the retention of the information and plans for its disposal once such information is no longer required for purposes of the Information Sharing Situation:**
7. **Specify the Party(s) who has custody or control of the information:**
8. **Other terms agreed to by the Parties:**

This Information Sharing Plan is effective **[insert date]** upon its signing by the Parties below.

[PARTY A]

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

[PARTY B]

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

[PARTY C]

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

[PARTY D]

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

[PARTY E]

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

[PARTY F]

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

[PARTY G]

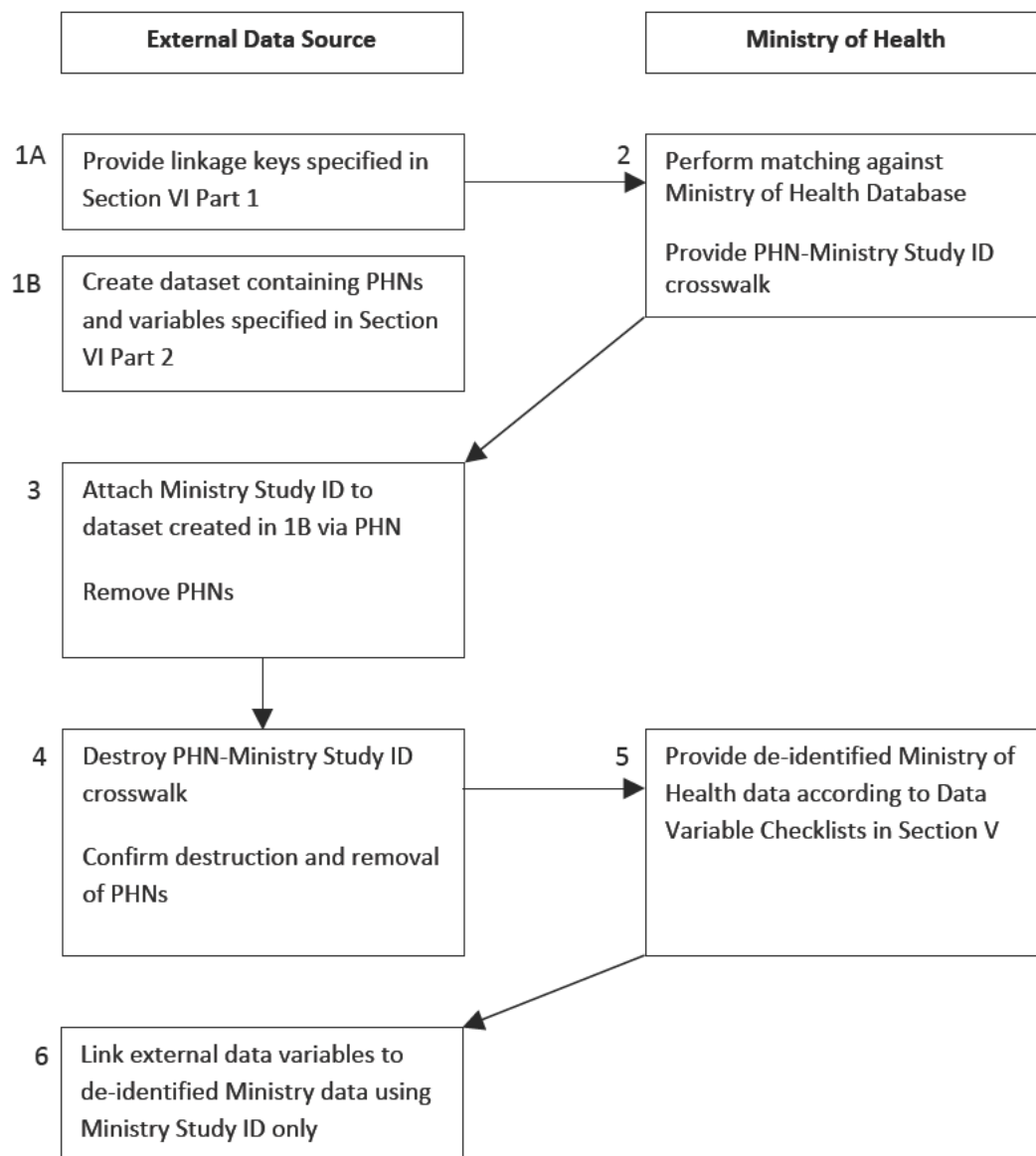
By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

Linkage Strategy A – cohort defined using External Data Source



See next page for step-by-step description

Step-by-Step:

Step 1A: External Data Source prepares and provides the Ministry of Health (the “Ministry”) an electronic data file consisting of all linkage keys of the cohort for linkage purpose only, specified in Section VI Part 1 Linkage Key Table of this application.

Step 1B: External Data Source prepares a version of the dataset to be used for the analysis of this project. This dataset should only contain the variables specified in Section VI Part 2 External Data Variables for Analysis of this application and the PHNs.

Step 2: The Ministry performs data matching and assigns Ministry study ID to the individuals in the cohort that are successfully matched. The Ministry sends PHN-to-Ministry study ID crosswalk file to External Data Source.

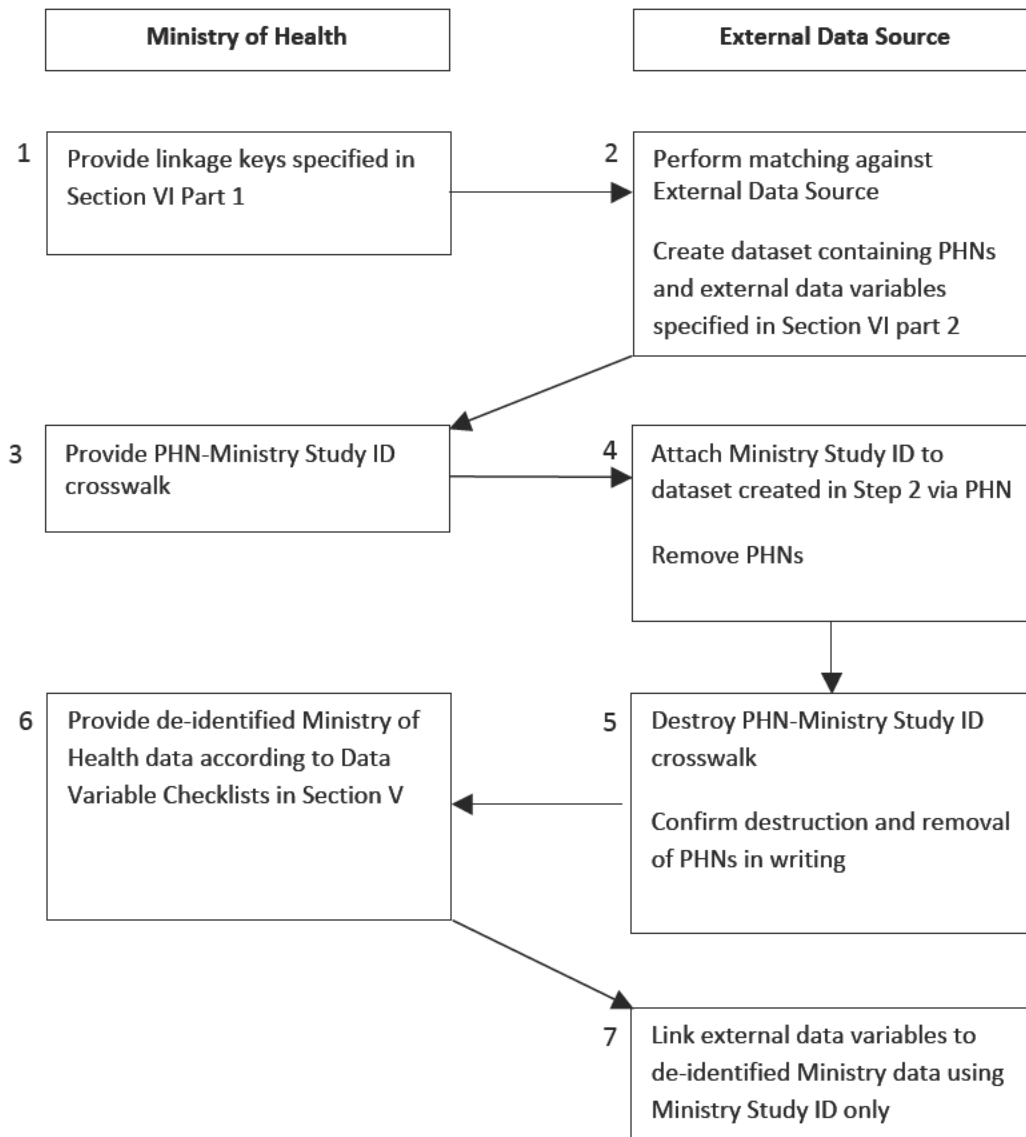
Step 3: External Data Source assigns Ministry study ID to the dataset prepared in Step 1B and removes PHNs.

Step 4: External Data Source destroys PHN-to-Ministry study ID crosswalk file and confirms with the Ministry in writing the destruction of crosswalk file and removal of PHNs.

Step 5: The Ministry prepares and provides de-identified Ministry data according to the Data Variable Checklist, specified in Section V of this application.

Step 6: External Data Source links files prepared in Step 3 and 5 via Ministry study ID only to carry out the analysis.

Linkage Strategy B for trusted partners – cohort defined using Ministry of Health data



See next page for step-by-step description

Step-by-Step:

Step 1: The Ministry of Health (the “Ministry”) prepares and provides External Data Source an electronic data file consisting of all linkage keys of the cohort for linkage purpose only, specified in Section VI Part 1 Linkage Key Table of this application.

Step 2: External Data Source performs matching of the cohort. External Data Source prepares a version of the dataset to be used for the analysis of this project. This dataset should only contain the variables specified in Section VI Part 2 External Data Variables for Analysis of this application and the PHNs.

Step 3: The Ministry sends PHN-to-Ministry study ID crosswalk file to External Data Source.

Step 4: External Data Source assigns Ministry study ID to the dataset prepared in Step 2 and removes PHNs.

Step 5: External Data Source destroys PHN-to-Ministry study ID crosswalk file and confirms with the Ministry in writing the destruction of crosswalk file and removal of PHNs.

Step 6: The Ministry prepares and provides de-identified Ministry data according to the Data Variable Checklist, specified in Section V of this application.

Step 7: External Data Source links files prepared in Step 4 and 6 via Ministry study ID only to carry out the analysis.

Ministry Internal Data Preparation Process

Roles

Data Analyst (Program Area)

Data linker (Open Data ICS - ODICS)

Secure LAN Dropbox

s. 15

Name of Dropbox

s.15

Data linkers and all data analysts have access to s.15 dropbox.

Data linkers have access to every dropbox.

Data analysts have access to their own dropbox.

Secure LAN Archive -

s. 15

Health Data Requests - Secure –

Archive

Data linkers archive all materials and copies of data and crosswalk. This is the permanent storage of all PI data related to each request. Access will be restricted to ODICS group only.

Sample File Naming Convention Guidelines

- Sample file name: 13-001_BCCDC_Varicella Schedule_Cohort
- Sample file name: 13-001_BCCDC_Varicella Schedule_MSP_2013-0135_A, 13-001_BCCDC_Varicella Schedule_MSP_2013-0135_B
- "A" always represents data file. "B, C, D" ...will represent look up files

Scenario 1a – MOH data only - one MOH database

- In accordance with the signed agreement, Data analyst prepares MOH data extract with PHN and places in program area secure dropbox using established naming conventions
- Data analyst emails data linker with cc to Health Authority Inbox (HealthDataHA@gov.bc.ca)
- Data linker replaces PHN in MOH data extract with corresponding study id
- Data linker encrypts MOH data extract and SFTPs to HA
- Data linker emails password to HA
- Data linker archives all data related files and emails Health Authority Inbox

Scenario 1b – MOH data only - multiple MOH databases

- In accordance with the signed agreement, Data analyst prepares MOH data extract with PHN and places in program area secure dropbox using established naming conventions
- Data analysts emails data linker with cc to Health Authority Inbox (HealthDataHA@gov.bc.ca)
- Once all data extracts are in secure dropbox, data linker combines PHNs from each data extract and creates a final list of cohort PHNs. Data linker creates PHN and Study ID crosswalk using the final list of cohort PHNs.
- Data linker replaces PHN in all MOH data extracts with corresponding study ID from crosswalk
- Data linker encrypts MOH data extracts and SFTPs to HA
- Data linker emails password to HA
- Data linker archives all data related files and emails Health Authority Inbox

Scenario 2 – Linking MOH data to HA data - cohort defined by HA

- Data linker receives list of cohort PHNs from HA through SFTP, places it into s.15 dropbox and notifies appropriate data analysts
- Data linker creates PHN and study ID crosswalk and SFTPs to HA
- In accordance with the signed agreement, Data analysts prepare MOH data extracts with PHN and place in appropriate program area secure dropbox using established naming conventions
- Data analysts email data linker with cc to Health Authority Inbox (HealthDataHA@gov.bc.ca)
- Once all MOH data extracts are in dropbox, data linker replaces PHN in all MOH data extracts with corresponding study id from crosswalk
- Upon receipt of written confirmation from HA of removal of PHNs and destruction of crosswalk file, data linker encrypts MOH data extracts and SFTPs to HA
- Data linker emails password to HA
- Data linker archives all data related files and emails Health Authority Inbox

Scenario 3 – Linking MOH data to HA data - cohort defined by MOH

- Data analyst prepares list of cohort PHNs according to signed agreement and place in s.15 dropbox using established naming conventions
- Data analyst notifies data linker with cc to Health Authority Inbox (HealthDataHA@gov.bc.ca)
- Data linker creates PHN and study ID crosswalk and SFTPs to HA
- In accordance with the signed agreement, Data analysts prepare MOH data extracts with PHN and place in appropriate program area secure dropbox using established naming conventions
- Data analysts email data linker with cc to Health Authority Inbox
- Once all MOH data extracts are in dropbox, data linker replaces PHN in all MOH data extracts with corresponding study id from crosswalk
- Upon receipt of written confirmation from HA of removal of PHNs and destruction of crosswalk file, data linker encrypts MOH data extracts and SFTPs to HA
- Data linker emails password to HA
- Data linker archives all data related files and emails Health Authority Inbox

GENERAL HEALTH INFORMATION SHARING AGREEMENT

This General Health Information Sharing Agreement (the "Agreement"), dated for reference June 1, 2013 (the "Effective Date"), is made AMONG:

HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA AS REPRESENTED BY THE MINISTER OF HEALTH

AND



("MOH")

FRASER HEALTH AUTHORITY

AND:

("FH")

VANCOUVER COASTAL HEALTH AUTHORITY

AND:



("VCH")

VANCOUVER ISLAND HEALTH AUTHORITY

AND:



("VIHA")

NORTHERN HEALTH AUTHORITY

AND:



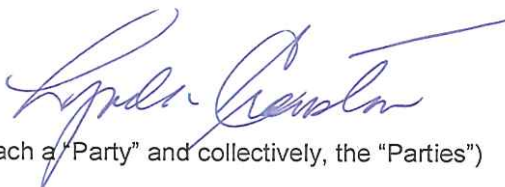
("NHA")

INTERIOR HEALTH AUTHORITY

AND:

("IHA")

PROVINCIAL HEALTH SERVICES AUTHORITY, British Columbia Cancer Agency, British Columbia Centre for Disease Control and Prevention Society, British Columbia Mental Health Society, British Columbia Transplant Society, Children's & Women's Health Centre of British Columbia, British Columbia Emergency Health Services, and Forensic Psychiatric Services Commission



("PHSA")

(each a "Party" and collectively, the "Parties")

BACKGROUND	4
1. INTERPRETATION.....	5
1.1 Definitions.....	5
1.2 Section references	9
1.3 Headings	9
1.4 Legislation	9
1.5 Schedules	9
2. SCOPE AND PURPOSE OF DATA SHARING	9
2.1 Agreement to Share	9
2.2 Scope and Methods of Sharing	9
2.3 Statutory Information Holdings	9
2.4 Existing Agreements	9
2.5 Exceptions	10
3. LEGAL/PRIVACY COMPLIANCE AND DATA PROTECTION	10
3.1 Public Body Status	10
3.2 Authorities for Collection, Use and Disclosure	10
3.3 Provision of Care	10
3.4 Secondary Use	10
3.5 Reasonable Security Precautions	13
3.6 Privacy Impact Assessments	13
3.7 Policies.....	14
3.8 Audit	15
3.9 Breach Investigations and Reporting	15
4. INFORMATION RIGHTS AND OBLIGATIONS	16
4.1 Discretion Regarding Party's Own Data	16
4.2 Accuracy	16
4.3 Compelled Disclosure	16
4.4 Access Requests	17
4.5 Right to Return of Information.....	17
4.6 Rights of Treating Parties	17
4.7 Access to Records for Legal Proceedings.....	17
5. GHISA SYSTEMS.....	17
5.1 GHISA Systems	17
5.2 Exclusions	17
5.3 GHISA System Categories	17
5.4 Terms Applicable to all GHISA Systems	18
5.5 Terms Applicable to Category B GHISA Systems	19
6. HEALTHCARE THIRD PARTIES.....	21
6.1 Service Providers	21
6.2 Private Healthcare Providers	21
6.3 Third Party Health Information Sources	21

7.	GOVERNANCE AND DISPUTE RESOLUTION	22
7.1	GHISA Steering Committee.....	22
7.2	Representatives	22
7.3	Dispute Resolution	22
8.	TERMINATION	22
8.1	Term.....	22
8.2	Termination.....	22
8.3	Transition	23
9.	GENERAL.....	23
9.1	Counterparts.....	23
9.2	Persons Bound	23
9.3	No Warranty.....	23
9.4	Indemnity	23
9.5	Further Assurances	23
9.6	Amendments	23
9.7	Survival	23
9.8	Assignment.....	23
9.9	Notices	24
9.10	No Fettering of Legislative Authority.....	25
9.11	Severability	25
	SCHEDULE A – Information Sharing Plan Template.....	27
	SCHEDULE B – Register of Category B GHISA Systems	31

BACKGROUND

A. MOH, under the Minister's direction, has a general mandate pursuant to the *Ministry of Health Act* to be in charge of all matters relating to public health, government-operated health insurance programs and healthcare stewardship generally within British Columbia (BC).

B. FH, VCH, VIHA, IHA and NHA are each health authorities within the meaning of the *Health Authorities Act*, each with a mandate to design, deliver and administer health care services within a designated geographic region of BC.

C. For the purposes of this Agreement, VCH includes Providence Health Care Society.

D. PHSA is a health care organization incorporated under the *Society Act*, with a mandate to provide specialized health care services and programs on a province-wide basis. For purposes of this Agreement, PHSA includes its branch societies, programs, services and entities managed by PHSA.

E. FH, VCH, VIHA, IHA, NHA and PHSA will be referenced herein collectively as "Health Authorities" and each as a "Health Authority".

F. MOH and the Health Authorities are public bodies within the meaning of the *Freedom of Information and Protection of Privacy Act* ("FIPPA") and are, therefore, governed by FIPPA, and other Applicable Laws in respect of their collection, use and disclosure of personal information.

G. All of the Parties currently share health information with or provide health information to each of the other Parties as well as with or to third parties for one or more the following purposes (each a "Healthcare Delivery & Related Purpose" and collectively, the "Healthcare Delivery & Related Purposes"):

- I. to provide care to patients or support the provision of care to patients, who may be transferred from one Health Authority's facility to another or are otherwise receiving care from two or more Health Authorities;
- II. to carry out joint programs and initiatives that seek to improve patient care in specialized healthcare areas;
- III. to study and analyze healthcare operations, administration, patient flow, patient movement across health authority boundaries, efficiency, effectiveness, costs, outcomes and other healthcare trends across the province with a view to improving the delivery of healthcare services in BC;
- IV. to facilitate and support health research;
- V. to establish health information systems to support and facilitate the sharing of health information between and amongst Health Authorities, MOH and third parties in connection with the delivery of, including the evaluation, monitoring and improvement of, healthcare services in BC;
- VI. to support public health programs and activities, including preventing the spread of communicable diseases, managing disease outbreaks, monitoring the overall health of people in BC and carrying out other duties under the *Public Health Act*;
- VII. to support activities related to the consolidation of corporate support and clinical support functions under the leadership of one Health Authority or other single entity as a means of deriving cost savings and efficiencies in the delivery of such services, including Lower Mainland Consolidation (LMC), a consolidation initiative of the Health Authorities which operate in the lower mainland of BC and Providence Health Care Society;

VIII. to allow MOH, its agents or service providers, to gather, compile, aggregate and/or analyze health data in order to conduct healthcare program evaluation, measure and monitor healthcare delivery performance, service availability and quality, engage in healthcare planning and improvement, including resource allocation and prioritization;

IX. to advance provincial healthcare initiatives, including public health initiatives, projects designed to improve healthcare efficiency, availability, quality and outcomes in one or more specific areas of care and establishment of electronic health information systems;

X. to otherwise support MOH activities required to carry out the Minister of Health's mandate under the *Ministry of Health Act* or otherwise, including with respect to inter-jurisdictional information-sharing arrangements relating to health that are entered by the Minister; and

XI. to support other Secondary Uses as defined in this Agreement.

H. The sharing of health information occurs through various methods including delivery of paper records, faxing, via telephone, delivery of electronic data on portable digital media, electronic data transmissions, access to each other's information systems and through common electronic information systems.

I. Historically, the Parties have entered into individual information sharing agreements where they deemed it necessary in order to support each health-related project, program, system or activity associated with a Healthcare Delivery & Related Purpose (each an "Information Sharing Situation"). MOH and the Health Authorities wish to enter into this Agreement in order to:

I. reduce the need to enter into individual agreements to support each Information Sharing Situation while still having in place the appropriate terms and conditions for each Information Sharing Situation with the proper level of specificity around access and security protocols in order to meet each Party's legal and privacy compliance obligations;

II. establish consistent, fundamental expectations and understandings around how information sharing for Healthcare Delivery & Related Purposes will be conducted, including a framework to ensure electronic information systems are used to facilitate information sharing and information management in a consistent, secure and privacy-compliant manner;

III. establish a governance framework for overseeing and making key decisions around information sharing activities; and

IV. create a trusted network amongst the Parties that facilitates information sharing for Healthcare Delivery & Related Purposes while ensuring that the information is protected and is only accessed, collected, used and disclosed for legally authorized purposes.

NOW THEREFORE, in consideration of the mutual covenants, promises and agreements contained in this Agreement, and other good and valuable consideration, the receipt and sufficiency of which is acknowledged, the Parties agree as follows:

AGREEMENT

1. INTERPRETATION

1.1 **Definitions.** The following terms in this Agreement, including any attached Schedules, will have the following meanings:

- (a) **"Applicable Laws"** means all statutes, ordinances, regulations, municipal by-laws, treaties, judgments and decrees applicable to any Party, property or event relating to this Agreement, including, without limitation, FIPPA.
- (b) **"Authorized User"** means an individual who is a member of a Party or Healthcare Third Party's Personnel and who has been duly granted access privileges to a GHISA System by a Party in accordance with the terms of this Agreement.
- (c) **"BC"** means the province of British Columbia.
- (d) **"Category A GHISA System"** has the meaning ascribed to that term in Section 5.3.
- (e) **"Category B GHISA System"** has the meaning ascribed to that term in Section 5.3.
- (f) **"Central Office"** has the meaning ascribed to that term in Section 5.5(c).
- (g) **"Common Access Management Framework"** has the meaning ascribed to that term under Section 5.5(a).
- (h) **"Consolidated Record"** means a Record containing Data collected, created or contributed to by multiple Parties and such Data is inextricably integrated such that it is not reasonably possible to identify the Party that collected or created it for purposes of separation and extraction.
- (i) **"Data"** means any health information and health-related information, including Personal Information and non-personally identifiable information:
 - (i) relating to the physical or mental health of an individual;
 - (ii) pertaining to the provision of health care to an individual, including the identification of a person as a provider of healthcare services to an individual or as a user of a system used to share health information; or
 - (iii) pertaining to health service delivery, including billing and insurance, budgeting, costing and financial planning or reporting, patient flow, wait times, outcomes, service quality, patient safety, healthcare trends and other information required for healthcare planning, evaluation and improvement,

in any form provided or disclosed by one Party to another for a Healthcare Delivery & Related Purpose. Data does not include employee information, such as an individual's employment record, used for the purpose of maintaining an employer-employee relationship or healthcare provider information used for the purpose of credentialing, privileging or maintaining service contracts, except to the extent such information is required in relation to auditing and managing employees or healthcare providers as it relates to their access to and use of health information shared under the GHISA.
- (j) **"Dataset"** means a collection of Data containing information pertaining to multiple individuals intended to be used for statistical analysis purposes.
- (k) **"Disclosing Party"** means a Party that discloses Data, including making such Data available for access via a GHISA System or otherwise, to a Receiving Party.
- (l) **"E-Health Act"** means the *E-Health (Personal Health Information Access and Protection of Privacy) Act*.

- (m) "FIPPA" means the *Freedom of Information and Protection of Privacy Act*.
- (n) "GHISA" means this General Health Information Sharing Agreement.
- (o) "GHISA Steering Committee" has the meaning ascribed to that term under Section 7.1.
- (p) "GHISA System" has the meaning ascribed to that term in Section 5.1.
- (q) "HA IMIS Policies" has the meaning ascribed to that term in Section 3.7(a).
- (r) "health information" means information relating to the physical or mental health of an individual, including information that consists of the health history of an individual's family.
- (s) "Health Information Privacy and Security Council" or "HIPSC" means the council consisting of privacy and security representatives from each of the Health Authorities, Providence Health Care Society and MOH, with a reporting relationship to the Health CIO Council, which currently meets once per month to discuss common privacy and information security issues, including developing common privacy practices to address similar issues across their respective organizations.
- (t) "Healthcare Delivery & Related Purpose" has the meaning ascribed to that term in Recital G.
- (u) "Healthcare Third Party" means an entity that is:
 - (i) a contracted service provider, including a provider of healthcare services under a service or affiliation agreement, to one or more of the Parties;
 - (ii) a provider of healthcare services within BC with which the Parties have traditionally shared health information in furtherance of one or more Healthcare Delivery & Related Purposes and with which the Parties agree to share Data under this Agreement;
 - (iii) a private sector medical laboratory which provides diagnostic testing services within BC;
 - (iv) an individual or organization which conducts health research and to which one or more of the Parties agree to release Data for such research in accordance with this Agreement, HA IMIS Policies and MOH IMIS Policies, as applicable, and Applicable Laws; or
 - (v) such other person as one or more of the Parties may agree to share Data with under the terms of this Agreement in furtherance of one or more of Healthcare Delivery & Related Purposes.
- (v) "Information Privacy Office" means the department within a Party's organizational structure that is responsible for leading and overseeing the Party's privacy compliance program.
- (w) "Information Sharing Plan" has the meaning ascribed to that term in Section 3.4(e).
- (x) "Information Sharing Situation" has the meaning given to it in Recital I.
- (y) "Inspected Party" has the meaning ascribed to that term in Section 3.8(a).

- (z) **"Inspecting Party"** has the meaning ascribed to that term in Section 3.8(a).
- (aa) **"MOH IMIS Policies"** has the meaning ascribed to that term in Section 3.7(b).
- (bb) **"patient"** means an individual receiving healthcare services and includes individuals commonly referred to a patient, client or resident.
- (cc) **"Personal Identifiers"** means any recorded information that could, either by itself or in combination with other information, be used to link or associate Personal Information to a particular individual (including but not limited to name, birth date, photograph, PHN, MRN, home address, postal code, personal telephone number, social insurance number (SIN), driver's license number, employee ID and other identity numbers).
- (dd) **"Personal Information"** means "personal information" as defined in FIPPA.
- (ee) **"Personnel"** means the officers, directors, employees, contractors, agents and representatives of a Party or Healthcare Third Party who collect, use or disclose Data and/or Records under this Agreement. For greater certainty, with respect to Health Authorities, physicians privileged to practice in a facility of a Health Authority will be considered a member of such Health Authority's Personnel to the extent they are engaged to provide healthcare services on behalf of the Health Authority.
- (ff) **"Private Healthcare Providers"** has the meaning ascribed to that term in Section 6.2.
- (gg) **"Receiving Party"** means a Party or Healthcare Third Party that receives Data, including via accessing a GHISA System or otherwise, from a Disclosing Party.
- (hh) **"Records"** means "records" as defined in FIPPA containing Data and to which access is granted by a Disclosing Party to a Receiving Party under the terms of this Agreement.
- (ii) **"Secondary Uses"** means all uses of Data for purposes other than direct provision of care to an individual or carrying out functions which support direct provision of care. For greater clarity, and without limiting the generality of the foregoing, Secondary Uses include all consistent uses of personal health information permitted under FIPPA, including s. 33.2(a), s. 34 and s. 35, and other Applicable Laws, such as program evaluation, quality improvement, healthcare planning, research, public health initiatives, system administration, medical education, privacy and security audits, and other incidental and reasonable uses of health information in connection with the delivery of health services other than for direct patient care of an individual.
- (jj) **"Statutory Information Holding"** means:
 - (i) a health information bank or ministry database established or designated under the E-Health Act,
 - (ii) prescribed information technology under the *Pharmaceutical Services Act*,
 - (iii) the health status registry continued under section 10 of the *Health Act*, or
 - (iv) any other health information registry, database or similar data holding, where a person is required by statute to disclose health information to that registry, database, or holding upon request.
- (kk) **"System Governance Framework"** has the meaning ascribed to that term in Section 5.5(b).

- (ll) **"System Owner"** means, in respect of a GHISA System, the Party that is the owner or licensee of the intellectual property rights in the system or otherwise has the right of control over the system vis-à-vis the other Parties.
- (mm) **"Third Party Information"** means information that is made available for access by Authorized Users or Personnel of the Parties and/or Healthcare Third Parties through a GHISA System or otherwise, which belongs to or is under the custody or control of an organization other than a Party.

1.2 **Section references.** Unless stated otherwise, capitalized section references refer to sections within this Agreement.

1.3 **Headings.** Headings are for reference and convenience only and shall not be interpreted as part of the substantive language of any provisions of this Agreement.

1.4 **Legislation.** Unless otherwise specified, each reference to a statute is deemed to be a reference to that statute and to regulations made under that statute, as amended or re-enacted from time to time, and each reference to a statute is a reference to a British Columbia statute.

1.5 **Schedules.** The following Schedules are attached to and form a part of this Agreement:

Schedule A – Information Sharing Plan Template

Schedule B – Register of Category B GHISA Systems

2. SCOPE AND PURPOSE OF DATA SHARING

2.1 **Agreement to Share.** As of the Effective Date and subject to the Section 4.1, the Parties agree relevant Data may be exchanged with each other and with Healthcare Third Parties as reasonably necessary for the furtherance of the Healthcare Delivery & Related Purposes in accordance with the terms and conditions set out in this Agreement and only as permitted under Applicable Laws.

2.2 **Scope and Methods of Sharing.** Subject to Sections 2.4 and 2.5, this Agreement shall govern all Data exchanges in connection with activities which further the Healthcare Delivery & Related Purposes regardless of the method of communication, including without limitation, delivery of paper records, faxing, via telephone, delivery of electronic data on portable digital media, electronic data transmissions and access to a GHISA System.

2.3 **Statutory Information Holdings.** The Parties acknowledge that Data may be shared between the Parties through or in connection with a Statutory Information Holding in furtherance of the Healthcare Delivery & Related Purposes. The Parties acknowledge that any such information exchange is subject to the specific statutory provisions applicable to the Statutory Information Holding and agree to fully comply with those provisions in respect of the collection, use and disclosure of the information, including when shared and accessed via a GHISA System.

2.4 **Existing Agreements.** Subject to Section 2.5, this Agreement will apply to all Data exchanges between the Parties in connection with the Healthcare Delivery & Related Purposes from the Effective Date. Agreements that were in effect prior to the Effective Date which govern existing Data exchanges ("Existing Agreement") between two or more of the Parties will continue to operate unless expired or the Parties involved agree to terminate such Existing Agreements and replace them with this Agreement. Where the Parties are uncertain as to the existence of an Existing Agreement governing a particular Information Sharing Situation or are unable to locate an Existing Agreement, the Parties involved may choose to rely on this Agreement to govern such Information Sharing Situation, including by creating an Information Sharing Plan in accordance with this Agreement, by mutual consent of the Parties involved. For greater certainty, where MOH is involved, an Information Sharing Plan will always be required to document such Information Sharing Situation.

2.5 **Exceptions.** To the extent that any provisions of this Agreement conflict with:

- (a) an information sharing agreement made under section 19 of the E-Health Act, subsection 5(5) of the *Medicare Protection Act* or section 41.1 of the *Vital Statistics Act*; or
- (b) the written limits and conditions referred to in section 24(2) of the *Pharmaceutical Services Act*; or
- (c) such other information sharing agreement mandated and regulated by Applicable Laws other than FIPPA

then such information sharing agreement or written limits and conditions will prevail.

3. **LEGAL/PRIVACY COMPLIANCE AND DATA PROTECTION**

3.1 **Public Body Status.** MOH and the Health Authorities are public bodies governed by the provisions of FIPPA and each Party is responsible for ensuring that, in discharging its obligations under this Agreement, it is fully compliant with FIPPA and other Applicable Laws.

3.2 **Authorities for Collection, Use and Disclosure.** The Parties will rely on such authority for collection, use and disclosure of Personal Information as may be applicable to a particular Information Sharing Situation. Where an Information Sharing Plan and/or privacy impact assessment are developed for a particular Information Sharing Situation, such documents will set out the appropriate authorities.

3.3 **Provision of Care.** Each Health Authority acknowledges and agrees that Data shared for direct provision of care or activities which support direct provision of care is based on the understanding that the Health Authority or the Healthcare Third Party and their Personnel accessing or receiving Data has a clinical relationship with or is otherwise involved in providing healthcare services to the individuals to whom the Data pertains. The Parties further acknowledge and agree that the Receiving Party and its Personnel may be required to confirm its clinical relationship with a particular individual, whether as an electronic acknowledge/confirmation within a GHISA System, or otherwise. Additionally, the Parties agree as follows:

- (a) **Case-by-case disclosures.** No further legal documentation is required beyond this Agreement when patient Records in paper format, including facsimiles, are transferred from one Health Authority to another on a case-by-case basis to support the care of the patients to whom such Records pertain. It is acknowledged that each Party as a public body is responsible for its compliance with FIPPA in respect of such Records that come into its custody or control.
- (b) **Disclosure via Systems.** Disclosure of Data for provision of care purposes via a GHISA System will be conducted in accordance with Article 5.

3.4 **Secondary Use.** The Parties agree as follows regarding using Data for Secondary Uses:

- (a) **Personal Identifiers.** The Parties acknowledge the following in respect of the use of Personal Identifiers for Secondary Uses:
 - (i) performing analysis and drawing conclusions based on data for research or other statistical studies does not generally require Personal Identifiers and concerted efforts should be undertaken to accomplish such activities using de-identified data; however, Personal Identifiers may be required in order to perform data linkage when analysis is being performed on data that is being combined from multiple sources or different time periods;

- (ii) Secondary Uses includes activity that, while being considered quality assurance and improvement in nature as opposed to direct patient care, is operational in nature and does require care providers and their managers to review actual patient records or other records in personally identifiable form often on a day-to-day basis, whether contained in a paper file or electronic health record, in order to ensure that care is being provided properly and to the expected standard of the program or services;
 - (iii) Secondary Uses such as system administration or medical education do not generally require Personal Identifiers to achieve the end goal of such activities, but individuals engaged in such activities may be exposed to or encounter Personal Identifiers incidentally as part of that activity; and
 - (iv) Secondary Uses such as health information management and data administration requires individuals engaged in such activities to handle personally identifiable information in order to perform their duties to manage and provide Data to those who require it and are authorized to receive it.
- (b) **Minimizing Access to Personal Identifiers.** Based on the acknowledgements in Section 3.4(a) and subject to Applicable Laws, the Parties agree that Data will be shared with each other or with Healthcare Third Parties for Secondary Uses in a manner that only discloses Personal Identifiers where reasonably required to achieve the intended purpose. Where it has been demonstrated that Personal Identifiers are required to be disclosed, protocols will be established to:
 - (i) limit access to Personal Identifiers to the minimum number of individuals involved who actually require access for activity such as data linkage;
 - (ii) minimize the number of Personal Identifiers which are disclosed; and
 - (iii) de-identify the data at the earliest possible stage in the data handling process.
- (c) **Data Retention.** Any Data provided to a Party in an Information Sharing Situation for Secondary Uses will be retained in accordance with the corresponding Information Sharing Plan. In the absence of an Information Sharing Plan and subject to Applicable Laws, the Data will be retained only until such time as the Information Sharing Situation has been concluded or the purpose for which such information was disclosed to the Party in connection with the Information Sharing Situation has been achieved, whichever is earlier.
- (d) **Research.** The Parties agree that the release of Data received by a Party under this Agreement to a third party for research purposes must only be done in accordance with Applicable Law such as section 35 of FIPPA, including entering into a research or information sharing agreement with such third party as required.
- (e) **Information Sharing Plans.** The Parties acknowledge that some Information Sharing Situations will involve the sharing of Data for one or more Secondary Uses using means other than by direct access to a GHISA System through a front-end interface (e.g., data extracts). In such Information Sharing Situations, where the applicable Parties consider it to be necessary and/or appropriate from a privacy compliance perspective, those Parties will create and document a plan for the proper and secure sharing of Data that suits the needs of the Information Sharing Situation ("Information Sharing Plan"). In assessing whether an Information Sharing Plan is necessary and/or appropriate, the Parties will consider the following factors:

- (i) the sensitivity and amount of the information involved;
- (ii) whether third parties are involved;
- (iii) the frequency and duration of the information sharing;
- (iv) whether there is an existing standard process in place for the type of disclosures contemplated; and
- (v) such other factors as the Parties deem relevant.

The Information Sharing Plan developed for each Information Sharing Situation will be in the format and contain the categories of information outlined in the Information Sharing Plan Template, attached as Schedule A to this Agreement, as may be amended from time to time by written agreement of the Parties thereto, but will at all times contain the following minimum information:

- (vi) a general description of the Information Sharing Situation, including the goals or objectives which the information sharing is intended to support;
 - (vii) the authorities under FIPPA and other Applicable Laws for collection, use and disclosure of Personal Information;
 - (viii) the categories of information being collected, used and shared, including specifying all or the main data elements where reasonably possible, and the reasons why such information needs to be collected, used and shared for purposes of the Information Sharing Situation;
 - (ix) the categories of individuals within each Party who are authorized to access the information, including whether access to Personal Information is permitted, and the reasons for their access;
 - (x) how the information will be shared, with whom (include data flow diagrams) and how it will be secured while in transmission and when in storage, including how access will be controlled;
 - (xi) the timeline(s) for the retention of the information and plans for its disposal once such information is no longer required for purpose of the Information Sharing Situation; and
 - (xii) the Party(s) who has custody or control of the information.
- (f) **Adherence to Information Sharing Plan.** Each Party involved in an Information Sharing Situation agrees to adhere to the corresponding Information Sharing Plan as approved by unanimous agreement of the Parties participating in the Information Sharing Situation.
 - (g) **Authorized Signatory for Information Sharing Plan.** Each Party will designate an individual who will act as its authorized signatory for each Information Sharing Plan. A Party may choose the same individual or different individuals for different Information Sharing Plans.
 - (h) **Stewardship Purposes under the *Ministry of Health Act*.** Where an agreed-to Information Sharing Plan involves the disclosure of Personal Information by a Health

Authority to the MOH for a "stewardship purpose" as defined in section 9 of the *Ministry of Health Act*, the Parties agree that:

- (i) MOH is authorized to collect such Personal Information from the Health Authority pursuant to section 26(a) of FIPPA and section 10(1)(a) of the *Ministry of Health Act*, and
- (ii) the Health Authority is authorized to disclose such Personal Information to the MOH pursuant to section 33.1(1)(c) and (d) of FIPPA, section 11 of the *Ministry of Health Act*, this Agreement and the Information Sharing Plan.

3.5 Reasonable Security Precautions. Each Party, both individually and collectively as part of any Information Sharing Situation, including in the operation and use of a GHISA System, agrees to take reasonable security measures to protect Data, whether stored on paper or in electronic format, that comes into its custody or control under this Agreement against unauthorized access, collection, use, disclosure or disposal in compliance with section 30 of FIPPA.

3.6 Privacy Impact Assessments. The Parties agree to conduct privacy impact assessments (PIAs) as required by FIPPA, including meeting all requirements under section 69 of FIPPA, and as needed to support various Information Sharing Situations, including the development of GHISA Systems.

- (a) **PIA Objectives.** The Parties agree that the main objectives of a PIA should be to:
 - (i) identify whether the legal authorities exist for the collection, use and disclosure of Personal Information as contemplated for the Information Sharing Situation;
 - (ii) identify the privacy and security risks and make recommendations to prevent or address them; and
 - (iii) establish accountabilities for implementation or compliance with the recommendations made under Section 3.6(a)(ii).
- (b) **PIA Recommendations.** PIA recommendations will be made in consideration of the following factors:
 - (i) recommendations shall be made which, if implemented, are designed to place the Parties involved in an Information Sharing Situation in full compliance with all requirements under FIPPA and other Applicable Laws;
 - (ii) subject to compliance with subsection (b)(i), recommendations should be practical, reasonable and effective in light of the circumstances, taking into account appropriate factors, including, but not limited to:
 - A. the degree of risk being addressed, having regard to the sensitivity of the information involved and the potential consequences of any accidental or unauthorized disclosure or use of such information;
 - B. the importance of the Information Sharing Situation in terms of contributing to the improvement of the delivery of healthcare services;
 - C. the ease/difficulty of implementation given the current environment, including workflow, workloads and technical environment;
 - D. costs and resources required to implement; and

- E. patient health and safety risks associated with a particular recommended course of action.
- (iii) recommendations should be designed to align the activity associated with an Information Sharing Situation against applicable HA IMIS Policies and MOH IMIS Policies, identify gaps and recommend solutions to address the gaps;
- (iv) recommendations should be designed to bring consistency in practices to Information Sharing Situations which are similar in nature; and
- (v) subject to subsections (b)(i) and (b)(ii), recommendations should strive to be consistent with industry standards for best privacy and security practices.
- (c) **Adherence to PIA Recommendations.** The Parties involved in a particular Information Sharing Situation shall use reasonable efforts to implement all the recommendations that are agreed to by the Parties in a PIA.
- (d) **Updating PIAs.** The Parties will revise and update PIAs as necessary to reflect and support changes to Information Sharing Situations.
- (e) **Common PIA Template.** The Parties will work toward the development of a single PIA template that will be used to assess Information Sharing Situations involving two or more of the Parties and such a template will be consistent with any directives of the Minister under section 69 of FIPPA.
- (f) **Lead Party.** In an Information Sharing Situation involving two or more of the Parties, the Parties involved will select a Party to lead the completion of the PIA (the "Lead PIA Party"). In selecting the appropriate Lead PIA Party, the Parties will consider which Party has the closest connection or greatest involvement to the Information Sharing Situation, including where the business/clinical leadership resides, i.e. the Party where the business/clinical leadership resides shall take the lead on the development of the PIA.
- (g) **When PIAs required.** The Parties will conduct a PIA for any Information Sharing Situation, unless the participating Parties deem it is not required in order to meet the Parties' obligations under FIPPA, including section 30. PIAs will generally be in new Information Sharing Situations which involve significant new activity in terms of the collection, use or disclosure of Personal Information, such as the creation of a new GHISA System or making significant modifications to an existing GHISA System. Where appropriate, the Parties may use an Information Sharing Plan, including the privacy analysis and assessments required to complete such a plan, to meet their obligations under FIPPA in place of a PIA. The decision as to whether a PIA is not required to be completed shall always be done in consultation with each Party's Information Privacy Office. Despite the foregoing, the Parties agree to comply fully with the requirement to conduct privacy impact assessments in accordance with section 69 of FIPPA.

3.7 Policies. Each Party will ensure that its relevant privacy and security policies, confidentiality undertakings and educational materials are consistent the Party's obligations under this Agreement. For greater certainty:

- (a) the Health Authorities will work to develop, adopt and implement common information management and information security (IMIS) policies, including policies governing access management, controls and audit, (collectively, "HA IMIS Policies") that are consistent with this Agreement, similar policies of the government of BC and the Common Access Management Framework and which provide greater detail and guidance to their respective Personnel to ensure compliance with the terms of this Agreement and with all

Applicable Laws in connection with their collection, use, disclosure and disposal of Data under this Agreement;

- (b) MOH will comply with the BC government's Information Security Policy and other policies pertaining to the same subject matter as the HA IMIS Policies (collectively, "MOH IMIS Policies"); and
- (c) where access by the Health Authorities to a GHISA System under the control of MOH requires that the Health Authorities comply with the MOH IMIS Policies, that obligation will be communicated in writing by the MOH in the applicable Information Sharing Plan for the Information Sharing Situation, the applicable System Governance Framework for that GHISA System, or otherwise.

3.8 Audit. The Parties agree as follows with respect to auditing and monitoring compliance with the terms and obligations of the Parties under this Agreement:

- (a) **Inspection.** In addition to any other rights of inspection that each of the Parties may have under this Agreement or under Applicable Laws, each Party shall permit any of the other Parties and/or its representatives and agents to conduct periodic audits related to performance by each Party of its obligations under this Agreement. Moreover, each Party seeking to inspect (the "Inspecting Party") may, at any reasonable time and on reasonable notice to another Party (the "Inspected Party"), enter on the other Party's premises to inspect any of the Data in the control of the Inspecting Party in the possession of the Inspected Party or any of the Inspected Party's information management policies or practices relevant to its management of the Data or its compliance with this Agreement.

For greater certainty, this Section 3.8(a) does not permit an Inspecting Party to inspect Data in the custody or control of an Inspected Party that is contained in a Statutory Information Holding, or that was required by law to be disclosed to the Inspected Party.

- (b) **Co-operation.** An Inspected Party shall co-operate, facilitate access to the Data, records and other relevant documentation and provide reasonable assistance to an Inspecting Party in conducting any investigation, audit, inquiry or in respect of any legal proceeding regarding non-compliance by the Inspected Party with this Agreement.
- (c) **Deficiencies.** If an audit identifies deficiencies in a Party's information management practices that affect compliance with any provision of this Agreement, or that affect the integrity of the Data, the Parties will initiate the procedures described in Section 3.9 of this Agreement.

3.9 Breach Investigations and Reporting. The Parties agree as follows with respect to investigating and reporting potential or actual privacy or security breaches:

- (a) **Investigation and Containment.** The Parties will cooperate and collaborate in the investigation of all cases, including identifying the appropriate Party to lead an investigation, where one or more of the Parties has reasonable grounds to believe that any of this Agreement's provisions regarding the Data has been or is likely to be breached, including deficiencies identified under Section 3.8(c) or any cases where it is alleged, suspected, or there is evidence, that there has been unauthorized access, use, disclosure or modification of the Data, or breach of confidentiality, or any incident which might jeopardize or has jeopardized the security or integrity of a Party's GHISA System. If a Party has any reasonable basis for suspecting that any Authorized User(s) may be utilizing access to a GHISA System in any manner or for purposes contrary to this Agreement, FIPPA or other Applicable Laws, that Party will or will cause the user's

access rights to be restricted or terminated as necessary to ensure the security of the information, including notifying the System Owner or Central Office as appropriate, during the course of the investigation.

- (b) **Report and Notice.** If any of the events detailed in Section 3.9(a) occur, the Party most closely connected to the events will immediately advise the other affected Parties, and provide a detailed written report of the circumstances of any unauthorized access, use, disclosure, modification, misuse or breach of confidentiality, or computer or network security breach and any remedial actions taken. Where determined, in consultation with the other affected Parties, to be appropriate by the Party which has custody or control of the information or system involved in the event, the Office of the Information and Privacy Commissioner of British Columbia (OIPC) and/or the individuals' whose information is affected may be informed, having due consideration to the breach reporting requirements/criteria established from time to time by the OIPC.
- (c) **Rectification.** Upon being notified under Section 3.9(b) of an instance of unauthorized access to, use, disclosure, modification, misuse, or breach of confidentiality respecting Data, or a breach regarding a GHISA System, a Party so notified may do any of the following:
 - (i) review the steps proposed by the Party(s) involved to address or prevent a recurrence of the non-compliance and direct that the Party(s) involved take the specified steps to prevent a recurrence. Such steps may include disciplinary action, suspension or termination of any Personnel that is involved by and at the sole discretion of the Party that maintains the employment or contractual relationship with that Personnel;
 - (ii) suspend the provision of Data under a particular Information Sharing Situation until satisfied the Party(s) involved has complied with the Agreement and any directions issued under Section 3.9(c)(i);
 - (iii) work collaboratively with the other affected Parties to take all reasonable steps to prevent recurrences of similar privacy or security breaches; or
 - (iv) terminate its participation in this Agreement, whether in whole or in regard to a particular Information Sharing Situation, in accordance with Article 8.

4. INFORMATION RIGHTS AND OBLIGATIONS

4.1 **Discretion Regarding Party's Own Data.** Despite any other provision in this Agreement, including Section 7.3, but subject to any Applicable Laws that mandate disclosure, each Party retains the discretion with respect to Data within its control to participate or decline to participate in an Information Sharing Situation for any reason, including on the basis that it does not have legal authority to disclose such Data or that such information sharing is prohibited under FIPPA, other Applicable Laws or a contractual obligation to which the Party is subject.

4.2 **Accuracy.** Subject to Section 9.3, the Parties will make reasonable efforts to provide accurate, complete, and up-to-date Data for all Data disclosures contemplated by this Agreement.

4.3 **Compelled Disclosure.** If a Party receives any demand, order, direction or is otherwise subjected to any requirement to disclose the Data or Records that are under the control of a Disclosing Party, that Party will promptly provide the Disclosing Party with notice of such demand or requirement together with full particulars thereof.

4.4 Access Requests. If a Party receives a request for access to the Data or Records under the control of the Disclosing Party, whether under Part 2 of FIPPA or otherwise, then that Party shall, subject to Applicable Laws, transfer or refer such request to the Disclosing Party. In the case of Consolidated Records or requests that capture the Data or Records under the control of two or more of the Parties, the Central Office, where applicable, or a Party designated by the affected Parties will administer the response and access management protocols in consultation with the other affected Parties.

4.5 Right to Return of Information. Subject to Sections 4.6 and 4.7, Article 8 and any applicable Information Sharing Plan and Applicable Law, upon request, each Party agrees to immediately return or destroy any Records, or any copies of such Records, shared by the requesting Party under this Agreement, unless:

- (a) the requesting Party was required by an enactment or its funding arrangement with the MOH to disclose such Records to the Party,
- (b) the Records are contained in a Statutory Information Holding, or
- (c) the Records are Consolidated Records in which case a Party will only be entitled to retain or retrieve a copy of such Consolidated Records pertaining to their patients beginning from the date in which the Party initially started participating in the creation of or contribution to the Consolidated Records or the earliest date associated with the Records that a Party has contributed to the Consolidated Records, whichever is earlier.

4.6 Rights of Treating Parties. Each Party using a Record obtained from another Party, whether through a GHISA System or otherwise, to make decisions about the care being provided to a patient (the "Treating Party") will have the right to retain a copy of such Record in paper or electronic format as part of the health record of the patient to whom the Record pertains. On inclusion of the copy of the Record in the patient's health record that resides in the custody or control of the Treating Party, that copy – but not the original Record – shall also be deemed to reside in the custody or control of the Treating Party, such that it may be further used or disclosed by the Treating Party as necessary, provided that such further use or disclosure is carried out in accordance with FIPPA and any other Applicable Law.

4.7 Access to Records for Legal Proceedings. Where an Authorized User has accessed a Record through a GHISA System in order to provide care to a patient or in a manner otherwise permitted under this Agreement, the Authorized User or the Party responsible for that Authorized User may request and be granted access to a read-only version of the original Record, including following termination of this Agreement, termination of the Party's participation in this Agreement, or suspension or termination of the Authorized User's access rights, provided that such access is demonstrably required in order to meet a statutory or regulatory requirement, or for use in connection with a legal proceeding in respect of which the Record meets the test of relevance.

5. GHISA SYSTEMS

5.1 GHISA Systems. The Parties agree that any electronic information system used to facilitate the sharing of Data amongst two or more Parties for a Healthcare Delivery & Related Purpose is considered a "GHISA System" for the purposes of this Agreement. For greater certainty, GHISA Systems include, without limitation, electronic health records, patient care information systems, provincial registries and portals into various source systems.

5.2 Exclusions. GHISA Systems excludes Statutory Information Holdings, but includes systems that may make Data from Statutory Information Holdings available to Authorized Users.

5.3 GHISA System Categories. GHISA Systems will be categorized as follows:

- (a) **Category A GHISA System** – a GHISA System that is only subject to the general terms and conditions for all GHISA Systems, as set out in Section 5.4; and
- (b) **Category B GHISA System** – a GHISA System that facilitates access to Data which originates from two or more Parties and in which all participating Parties agree that, in addition to the terms and conditions set out in Section 5.4 for all GHISA Systems, such system will also be subject to the terms and conditions applicable to Category B GHISA Systems, as set out in Section 5.5.

All GHISA Systems will be considered Category A GHISA Systems unless and until designated as a Category B GHISA System by approval of the GHISA Steering Committee.

5.4 Terms Applicable to all GHISA Systems. The following terms and conditions apply to all GHISA Systems:

- (a) **Access and Security Obligations.** The Parties acknowledge that, under the terms of this Agreement, each Party may be granted access to Personal Information of a highly sensitive nature, and each Party agrees as follows in respect of GHISA Systems used to share Data under this Agreement:
 - (i) **Access Model.** The Parties agree that access privileges for a GHISA System will be granted to Authorized Users in accordance with an access model that is minimally based on such users' "need to know" and/or "need to access" in order to perform their job duties and that is fully compliant with FIPPA.
 - (ii) **Authorized User Obligations.** Each party will:
 - A. take all reasonable measures to ensure that no access to the system, inadvertent or otherwise, is provided to any person other than an Authorized User;
 - B. comply with and cause all Authorized Users to comply with any restrictions, license terms or policies as reasonably determined by the System Owner, and any third party rights therein, all as may be notified in writing by the System Owner to the Party;
 - C. cause all Authorized Users to agree to a written undertaking, terms of use or agreement, whether on paper or in electronic format, consistent with the Party's obligations under this Agreement;
 - D. ensure that Authorized Users access and use Data only for purposes permitted by FIPPA and by this Agreement; and
 - E. ensure that there is no transfer of Personal Information outside of Canada, and that there is no access, remote or otherwise, to a GHISA System from any location outside of Canada, unless authorized by FIPPA and done in accordance with the applicable policies of the System Owner.
- (b) **Securing Passwords.** Each Party is responsible for ensuring the security of any devices, user IDs, codes or passwords it provides to its Authorized Users to enable access to Data and GHISA Systems.
- (c) **Third Party Information.** Each Party acknowledges that certain GHISA Systems may make Third Party Information available for access by Authorized Users. Each Party

agrees that none of the other Parties make any representations or warranties regarding Third Party Information made available via a GHISA System. The use of Third Party Information is subject to such third party terms and conditions as may be communicated in writing by the applicable System Owner or Central Office to the Parties accessing such information, unless otherwise expressly stated in this Agreement.

- (d) **Duty to Notify Authorized Users.** Each Party, working in cooperation with the Central Office, shall properly advise all its Authorized Users of its and their obligations under this Agreement and any existing information sharing agreements in force at the time this Agreement is signed, FIPPA and Applicable Laws.
- (e) **Availability of Systems.** Subject to Section 9.3, the Parties will make reasonable efforts to ensure any GHISA Systems to which electronic access rights have been granted hereunder are stable and available to the Receiving Parties.

5.5 Terms Applicable to Category B GHISA Systems. In addition to the terms and conditions set out in Section 5.4, the following additional terms and conditions apply to Category B GHISA Systems:

- (a) **Common Access Management Framework.** The access model for Category B GHISA Systems will be made consistent with a common access management framework (the "Common Access Management Framework") approved by the GHISA Steering Committee. The Framework will consist of a set of principles, approaches and rules that lay the foundation for how access to Category B GHISA Systems will be enabled, controlled and managed, including:
 - (i) a common approach to assigning access privileges to users, including role-based access;
 - (ii) common approaches to privacy controls such as disclosure directives, masking, enhanced information security, clinical relationship attestation and access to highly sensitive information; and
 - (iii) a common approach to access to and the release of Data from Category B Systems for Secondary Uses, including research in accordance with section 35 of FIPPA.

The Parties agree to develop the Common Access Management Framework using existing protocols, guidelines, frameworks and other related documentation that the Parties may have to support the access control and management needs of Category A and B GHISA Systems. The Parties acknowledge that each Party's obligation to implement the requirements and standards set out in the Common Access Management Framework is subject to available funds and resources required to implement changes to existing systems and processes. The GHISA Steering Committee, in consultation with appropriate stakeholders, will make decisions with respect to the timelines for the development, adoption and implementation of the Common Access Management Framework with respect to Category B GHISA Systems.

- (b) **System Governance Framework.** For each Category B GHISA System, the Parties will develop a document that sets out details with respect to the governance of the system and the Data contained in or made accessible through such system (a "System Governance Framework"). The System Governance Framework will contain the level of detail required for each particular situation, as agreed between the participating Parties, and may include:
 - (i) A description of the general purpose(s) of the system;

- (ii) The System Owner(s);
 - (iii) The Parties and Healthcare Third Parties that input their Data into or make their Data available via the system;
 - (iv) The Parties and Healthcare Third Parties that have access to the system;
 - (v) The designated Central Office for the system;
 - (vi) The Party(s) that has custody or control of the Data contained in or made accessible through the system;
 - (vii) The data steward or person or group of persons responsible for making decisions with respect to whether Data contained in or made accessible through the system should be provided or made accessible to a particular user, group of users or data requestor;
 - (viii) The process for obtaining access privileges into the system or obtaining Data from the system for both provision of care and Secondary Uses;
 - (ix) Whether the system is subject to HA IMIS Policies or MOH IMIS Policies or equivalent policies of the Central Office; and
 - (x) Other information deemed appropriate or required by the participating Parties.
- (c) **System Administration.** For Category B GHISA Systems, the participating Parties will select an organization, which may or may not be a Party, to be primarily responsible for the operation, maintenance and support of the system (the "Central Office") for the benefit of all the Parties involved in using said system to exchange Data. The Parties may enter into other agreements with each other, or with another organization where the Central Office is a not a Party to this Agreement, as to service quality, service levels, costs, intellectual property and other aspects regarding the delivery of system administration services by the Central Office and which is consistent with the responsibilities of the Central Office as set out in this Agreement. Unless otherwise agreed by the participating Parties, as may be reflected in the applicable System Governance Framework, the responsibilities of the Central Office for a Category B GHISA System will include, but may not be limited to, the following:
- (i) administering access to the GHISA System in accordance with the Common Access Management Framework and/or in accordance with applicable HA IMIS Policies or MOH IMIS Policies as developed and adopted by the Parties, including:
 - A. provisioning and de-provisioning user accounts; and
 - B. keeping current access profiles for all Authorized Users and ensuring that access privileges are updated in accordance with changes in Authorized User responsibilities and employment status.
 - (ii) performing or assisting with the performance of data release management functions in respect of data requests for Secondary Uses, all in accordance with applicable HA IMIS Policies or MOH IMIS Policies and this Agreement;

- (iii) taking reasonable measures to protect Data stored in or made accessible through the GHISA System against unauthorized access, collection, use, disclosure or disposal;
 - (iv) taking reasonable steps to manage, maintain and operate the GHISA System to make it available for use by Authorized Users as the system is intended to be used; and
 - (v) working with the applicable Parties to develop and implement appropriate audit mechanisms, procedures and protocols for monitoring access to Data in the GHISA System or available through the GHISA System and investigating and responding to actual or suspected instances of unauthorized access and other privacy breaches, including suspending or terminating the access of Authorized Users if necessary, all in accordance with Sections 3.8, 3.9 and 5.5(d).
- (d) **Auditing Access to GHISA Systems.** The Parties will cooperate in the development of common audit and breach investigation and response methods and procedures to detect, deter, investigate and respond to unauthorized access to and use of Category B GHISA Systems that are consistent with the terms for audit and breach investigations set out in Sections 3.8 and 3.9.
- (e) **GHISA Systems Register.** The Parties will create a register of Category B GHISA Systems in Schedule B to this Agreement, to be unanimously approved by the GHISA Steering Committee, to which the specific provisions relating to Category B GHISA Systems under this Agreement apply.

6. HEALTHCARE THIRD PARTIES

6.1 **Service Providers.** Each Party will ensure, whether through a service agreement/privacy schedule, affiliation agreement or other type of written contract, that its service providers who may have access to Data obtained from another Party under this Agreement are under an obligation to protect such information from unauthorized access, use and disclosure and to otherwise comply with the terms of this Agreement, as they may be reasonably applicable to the service provider, and that their Personnel are bound as though they were Personnel of the Party engaging such service provider.

6.2 **Private Healthcare Providers.** Where a Health Authority shares Data, as reasonably required to ensure continuity of care, with healthcare providers, including physicians and their staff in private practice, who provide healthcare services to patients of the Health Authorities, such services being provided to the patients in the providers' own capacities and not on behalf of the Health Authorities ("Private Healthcare Providers"). Such sharing will be consistent with Section 3.3 and may be done through the granting of access privileges to a GHISA System. If access is being provided to a GHISA System, Private Healthcare Providers will be required to sign the appropriate data access or information sharing agreement, which will require them to be bound by terms and obligations substantially similar to the terms and obligations imposed on the Parties and their Personnel for the protection and the appropriate use and disclosure of Data shared under this Agreement.

6.3 **Third Party Health Information Sources.** The Health Authorities acknowledge the value of health information in the possession of organizations and persons other than the Parties, including but not limited to medical laboratories and Private Healthcare Providers (collectively, "Third Party Health Information Sources"). Health and medical records created by such Third Party Health Information Sources are currently provided to Health Authorities in connection with the provision of care to common patients generally on a case-by-case and *ad hoc* basis and mostly through delivery of paper records or facsimile as part of the continuity of care as patients seek treatment and services from Health Authority facilities. The Parties acknowledge that efforts are underway to make health information from Third Party Health Information Sources more accessible to Personnel of Health Authorities and various Healthcare Third Parties through GHISA Systems in order that such information may be used to provide, more

effective care to the patients to whom such information pertains. The applicable Parties will agree on a case-by-case basis whether to proceed with any such initiatives and, if unanimous approval is granted, then the applicable Parties will enter into separate agreements with such Third Party Health Information Sources to govern the collection, use and disclosure of such Data, the terms and conditions of which shall be consistent with the terms and conditions of this Agreement.

7. GOVERNANCE AND DISPUTE RESOLUTION

7.1 GHISA Steering Committee. The Parties will establish a committee known as the General Health Information Sharing Agreement Steering Committee, a subcommittee of the Health CIO Council, consisting of one senior representative from each of the Parties (the "GHISA Steering Committee"), which will function as follows:

- (a) The GHISA Steering Committee will provide oversight and general governance over the administration, implementation and compliance with the terms and conditions of this Agreement.
- (b) The GHISA Steering Committee may invite non-voting individuals, such as subject matter experts, to attend the Committee's meetings to help inform their discussions and decisions.
- (c) Decisions made by the GHISA Steering Committee are subject to Section 4.1.

7.2 Representatives. Each of the Parties shall appoint, and make available, a representative(s) to facilitate communications between the Parties regarding any dispute, issue, incident, complaint or other concerns arising in connection with the Data exchanges and other activities and practices contemplated by this Agreement (the "Representatives").

7.3 Dispute Resolution. The Parties agree to work together in good faith to resolve any disputes arising under this Agreement. Any disputes arising between the Parties will first be raised between their respective Representatives appointed in accordance with Section 7.2 above, or if the Parties involved agree, bring it forward for discussion and resolution at HIPSC. If the Representatives are unable to resolve any dispute between them within 30 days of having reasonable opportunity to consider the issue, then the issue shall be brought forward to the GHISA Steering Committee for discussion and resolution. If no resolution is reached within a further 30 days after the GHISA Steering Committee has had reasonable opportunity to consider the issue, then the Parties shall refer the matter to their respective Chief Executive Officers, in the case of the Health Authorities, and the Deputy Minister of Health, in the case of the Ministry of Health, for resolution. If no resolution is reached within a further 30 days after the Chief Executive Officers and the Deputy Minister of Health have had a reasonable opportunity to consider the issue, then the matter shall be referred to and settled by the Minister of Health.

8. TERMINATION

8.1 Term. Notwithstanding the date of execution and delivery of this Agreement, the term of this Agreement will commence on the Effective Date and it shall continue for a period of 10 years from that date unless sooner terminated in accordance with this Article.

8.2 Termination. This Agreement may be terminated in the following manner:

- (a) this Agreement may be terminated at any time, subject to Section 8.3, with the written agreement of all of the Parties; or
- (b) a Party may terminate its participation (i) in this Agreement on providing 90 days written notice to all the other Parties, or (ii) in a specific Information Sharing Situation on providing 30 days written notice to the other Parties involved.

8.3 Transition. Upon the termination of this Agreement or the termination of a Party's participation in this Agreement or a particular Information Sharing Situation, the Parties involved will work together to develop a mutually agreeable transition plan to address any Data sharing, GHISA Systems or management issues arising from the termination of this Agreement or any access privileges granted under this Agreement, including without limitation the return or the secure disposal/destruction of Data and Records by each Receiving Party at the option of the Disclosing Party. With respect to Consolidated Records, each Party shall be entitled to retain or retrieve a copy of such records for their patients dating back to the date in which the Party commenced participating in the creation of or contributing to the Consolidated Records.

9. GENERAL

9.1 Counterparts. This Agreement may be executed in any number of counterparts, including electronically produced copies, each of which will be deemed to be an original and all of which taken together will constitute one agreement.

9.2 Persons Bound. This Agreement will enure to the benefit of and be binding upon the Parties and their lawful successors and permitted assigns.

9.3 No Warranty. Notwithstanding Sections 4.2 and 5.4(e), the Data exchanged under this Agreement and the availability of access to a GHISA System is provided on an "as is", "where is" and "as available" basis. Except as expressly set out in this Agreement and except where agreed in writing between the applicable Parties to the contrary, the Parties expressly disclaim and will not be bound by any express, implied, statutory or other warranty, representation or condition in respect of such Data or GHISA Systems, including without limitation warranties, representations or conditions of merchantable quality, uninterrupted or error-free access, accuracy or completeness of data, availability, non-infringement, or fitness for a particular purpose.

9.4 Indemnity. For the purpose of this Section, "Loss" means costs, losses, damages, liabilities and expenses (including all reasonable legal costs, fees and disbursements). Each Party (the "Indemnifying Party") will indemnify and hold harmless every other Party, its officers, employees and its agents (each an "Indemnified Party") for any and all Loss resulting directly or indirectly from the breach of this Agreement by the Indemnifying Party, its officers, employees or agents, except to the extent that such Loss arises from an independent breach of this Agreement by another Party. This indemnity will survive the termination of this Agreement. An Indemnified Party must take all reasonable steps to minimize the Loss it has suffered or is likely to suffer as a result of the event giving rise to an indemnity under this Section.

9.5 Further Assurances. The Parties will execute and deliver to each other any further instruments and do any further acts that may be required, including the creation or amendment of internal policies and procedures, to give full effect to the intent expressed in this Agreement.

9.6 Amendments. This Agreement may not be modified except by an agreement in writing signed by all the Parties.

9.7 Survival. Provisions that are by their nature intended to continue following termination of this Agreement shall survive the termination of this Agreement, including without limitation, Sections 3.9, 4.4, 4.7, 8.3, 9.4 as well as each Party's obligations to comply with FIPPA and to ensure that its Personnel maintain the confidentiality of Data exchanged under this Agreement.

9.8 Assignment. A Party may not assign any of its rights under this Agreement without the prior written consent of the other Parties, and any purported assignment without such prior written consent will be void and of no force or effect.

9.9 **Notices.** All notices under this Agreement will be in writing and may be sent by overnight courier, pre-paid courier, by facsimile (receipt confirmed by the receiving fax), or by electronic mail to the following addresses:

- For MOH: Ministry of Health**
2-1 1515 Blanshard Street, Victoria BC, V8W3C8
Attention: Chief Data Steward
Fax: 250-952-2002
Email: shirley.wong@gov.bc.ca
- For FH: Fraser Health Authority**
Suite 100, Central City Tower, 13450 – 102nd Avenue, Surrey, BC, V3T 5X3
Attention: Manager, Information Privacy
Fax: 604-953-5157
Email: seana-lee.hamilton@fraserhealth.ca with copy to privacy@fraserhealth.ca
- For VCH: Vancouver Coastal Health Authority**
11th Floor, 601 West Broadway, Vancouver, BC, V5Z 4C2
Attention: General Legal Counsel & Chief Privacy Officer
Fax: 604-875-4593
Email: steven.tam@vch.ca or privacy@vch.ca
- For VIHA: Vancouver Island Health Authority**
Executive Office, Royal Jubilee Hospital, Begbie Hall
1952 Bay Street, Victoria, BC V8R 1J8
Attention: Chief Information Officer
Fax: 250-370-8750
Email: catherine.claiterlarsen@viha.ca
- For NHA: Northern Health Authority**
Suite 600 - 299 Victoria Street, Prince George, BC, V2L 5B8
Attention: Vice President / Planning, Quality and Information Management
Fax: 250-565-2640
Email: Fraser.Bell@northernhealth.ca
- For IHA: Interior Health Authority**
Capri Centre, #200 – 1835 Gordon Drive, Kelowna, BC, V1Y 3H5
Attention: Director, Technology Architecture & Services and Information Privacy & Security
Fax: 250-491-6789
Email: mark.braidwood@interiorhealth.ca
- For PHSA: Provincial Health Services Authority**
700 – 1380 Burrard Street, Vancouver, BC, V6Z 2H3
Attention: General Legal Counsel, Chief Enterprise Risk & Privacy Officer
Fax: 604-675-7229
Email: leon.bresler@phsa.ca

Proof of delivery in the above manner will constitute proof of receipt. Any Party may designate different contact information by giving the other Parties written notice of the new information.

9.10 **No Fettering of Legislative Authority.** Nothing in this Agreement will be construed as an agreement by MOH to restrict, limit or otherwise fetter in any manner the MOH's ability to introduce, pass, amend, modify, replace, revoke or otherwise exercise any rights or authority regarding legislation, regulations, orders, policies or any other authority of the MOH.

9.11 **Severability.** If any provision of this Agreement is held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions will not in any way be affected or impaired, and will be interpreted in the context of the remaining provisions.

IN WITNESS WHEREOF this Agreement takes effect as of the Effective Date upon its signing by the respective authorized representatives of the Parties.

MINISTRY OF HEALTH

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

FRASER HEALTH AUTHORITY

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

VANCOUVER ISLAND HEALTH AUTHORITY

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

NORTHERN HEALTH AUTHORITY

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

9.10 **No Fettering of Legislative Authority.** Nothing in this Agreement will be construed as an agreement by MOH to restrict, limit or otherwise fetter in any manner the MOH's ability to introduce, pass, amend, modify, replace, revoke or otherwise exercise any rights or authority regarding legislation, regulations, orders, policies or any other authority of the MOH.

9.11 **Severability.** If any provision of this Agreement is held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions will not in any way be affected or impaired, and will be interpreted in the context of the remaining provisions.

IN WITNESS WHEREOF this Agreement takes effect as of the Effective Date upon its signing by the respective authorized representatives of the Parties.

MINISTRY OF HEALTH

By: 
(Signature of Authorized Signatory)
Name: Graham Williams
(Printed)
Title: DM HEALTH
Date: 27/5/13

FRASER HEALTH AUTHORITY

By: _____
(Signature of Authorized Signatory)
Name: _____
(Printed)
Title: _____
Date: _____

VANCOUVER ISLAND HEALTH AUTHORITY

By: _____
(Signature of Authorized Signatory)
Name: _____
(Printed)
Title: _____
Date: _____

NORTHERN HEALTH AUTHORITY

By: _____
(Signature of Authorized Signatory)
Name: _____
(Printed)
Title: _____
Date: _____

INTERIOR HEALTH AUTHORITY

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

VANCOUVER COASTAL HEALTH AUTHORITY

By: _____
(Signature of Authorized Signatory)

Name: Dr. David Ostrow
(Printed)

Title: President & CEO

Date: May 16, 2013

**PROVINCIAL HEALTH SERVICES AUTHORITY, on
its own behalf and on behalf of BRITISH COLUMBIA
CANCER AGENCY, BRITISH COLUMBIA CENTRE
FOR DISEASE CONTROL AND PREVENTION
SOCIETY, BRITISH COLUMBIA MENTAL HEALTH
SOCIETY, BRITISH COLUMBIA TRANSPLANT
SOCIETY, CHILDREN'S & WOMEN'S HEALTH
CENTRE FOR BRITISH COLUMBIA, BRITISH
COLUMBIA EMERGENCY HEALTH SERVICES, and
FORENSIC PSYCHIATRIC SERVICES COMMISSION**

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

SCHEDULE A

INFORMATION SHARING PLAN TEMPLATE

This Information Sharing Plan (ISP) must be completed in consultation with the Information Privacy Offices of the Parties involved in the Information Sharing Situation this ISP is intended to cover. When completed and approved by each of the participating Parties, this (ISP) forms part of and is subject to the terms and conditions of the General Health Information Sharing Agreement (GHISA). Capitalized terms will have the same meaning as defined in the GHISA.

1. **Description of Information Sharing Situation, including the goals or objectives which the information sharing is intended to support:**

2. **Authorities for Collection, Use and Disclosure under FIPPA and other Applicable Laws:**

Section references are to FIPPA unless otherwise specified.

Collection – Authorities for collection for the parties collecting personal information:

- ☐ **Section 26(a)** – authorized expressly by a law

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

- ☐ **Section 26(c)** – necessary for operating program

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

- ☐ **Section 26(e)** – necessary for planning or evaluating a program or activity of a public body

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

- ☐ **Section 27(1)(a.1)** – indirect collection necessary for medical treatment and it is not possible to collect the information directly from the individual or obtain authority for another method of collection

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

- ☐ **Section 27(1)(b)** – indirect collection from another public body which is disclosing the information under sections 33 to 36

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

- ☐ **Section 27(1)(e)** – necessary for delivering or evaluating a common or integrated program or activity

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Other Applicable Law(s)/section(s):** _____

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

Use – Authorities for use for the parties using personal information:

☐ **Section 32(a)** – use for purpose for which it was collected or compiled

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 32(b)** – use for which the individual has consented

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 32(c)** – use for purpose for which it was disclosed to the public body under ss. 33 to 36

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Other Applicable Law(s)/section(s):** _____

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

Disclosure – Authorities for disclosure for the parties disclosing information:

☐ **Section 33.2(a)** – disclosure for original purpose of collection or consistent purpose

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 33.2(d)** – common or integrated program or activity

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 33.2(l)** – necessary for planning or evaluating a program or activity of a public body

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 33.1(c)** – disclosure authorized or required by an enactment of BC (other than FIPPA) or Canada

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Section 33.1(1)(e.1)** – disclosure to service provider

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

☐ **Other Applicable Law(s)/section(s):** _____

Applicable to: ☐ FHA, ☐ IHA, ☐ NHA, ☐ PHSA, ☐ VCH, ☐ VIHA ☐ MOH

For:

3. **Specify the categories of information being collected, used and shared, including specifying all or the main data elements where reasonably possible and, in the case of each data element, the reasons why such information needs to be collected, used and shared for purposes of the Information Sharing Situation:**
4. **Specify the categories of individuals within each Party who are authorized to access the information, including whether access to Personal Information is permitted, and the reasons for their access:**
5. **Specify how the information will be shared, with whom(include data flow diagrams) and how it will be secured while in transmission and when in storage, including how access will be controlled:**
6. **Specify the timeline(s) for the retention of the information and plans for its disposal once such information is no longer required for purposes of the Information Sharing Situation:**
7. **Specify the Party(s) who has custody or control of the information:**
8. **Other terms agreed to by the Parties:**

This Information Sharing Plan is effective [insert date] upon its signing by the Parties below.

[PARTY A]

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

[PARTY B]

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

[PARTY C]

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

[PARTY D]

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

[PARTY E]

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

[PARTY F]

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

[PARTY G]

By: _____
(Signature of Authorized Signatory)

Name: _____
(Printed)

Title: _____

Date: _____

SCHEDULE B

REGISTER OF CATEGORY B GHISA SYSTEMS

No.	NAME OF SYSTEM	CENTRAL OFFICE	DATE APPROVED



MINISTRY OF HEALTH
DATA EXTRACT SCHEDULE TO DATA ACCESS
AGREEMENT

DATA ACCESS AGREEMENT NO: 2012_XX
ORGANIZATION NUMBER: 1763

Title:

Background

The [Health Authority [i.e. Interior Health Authority; hereafter, "IHA"]] has requested access to [Medical Service Plan (MSP), Discharge Abstract Database (DAD), etc.] records for [insert region] (the "Data").

*This section identifies the context/***importance** *of the analysis and provides a brief background for the types of data requested, for example: This program was created as an initiative of this organization to evaluate health outcomes related to this chronic condition which affects several individuals annually.*

If conducting a program evaluation, name and describe the program.

Purpose:

NOTE: The purpose must identify an objective clearly related to the data request (i.e. assessment of a surveillance method, specific program evaluation, etc.) A request for data "in support of decision-making and service planning" will not suffice.

1. Specific Request for Data Access

This Schedule to the Agreement (the "Schedule") between the IHA and the BC Ministry of Health (the "Ministry"), dated December 7, 2002, with extensions, sets out specific terms for the IHA to access [MSP, DAD, etc.] for the years [enter specific date range].

IHA must not use Data disclosed under this Schedule to identify or contact any individual.

If the data request involves a specific study population (i.e. a cohort), please describe.

2. Methods of Access

- a) The data sender will provide the data receiver with either a password protected CD, or transfer the data files using a secure method such as the Secure File Delivery System or Secure File Transport Protocol that contains the data elements specified in Section 12 of this Schedule. All outgoing CD's will be password encrypted and a two-step process (one envelope containing the CD and the next letter or e-mail containing the password - If a password is send on a CD, the CD is sent separately in a sealed envelope using Rush and Trace). Software required to enable encryption such as Win Zip Self Extractor should be used with a minimum of 256 bit encryption using Advanced Encryption Standard; randomly generated minimum 64 digit password using a

combination of at least one uppercase, one lower case, and one number and may contain symbols.

- b) Passwords (if applicable) will be provided under separate cover and preferably by separate methods.

3. Data to be Disclosed

The IHA is requesting [*one-time*] access to de-identified, record-level [DAD, MSP, etc] data for the above purpose. The specific data elements requested are included in Section 12 of this Schedule.

The IHA is requesting data from [date range] (*state either calendar or fiscal year*)

[name, position, IHA], is the individual responsible for receiving the Data.
[name, position, IHA], of individuals accessing the Data.

4. Use of Data

IHA is permitted to use these data for the Purpose indicated above only.

IHA must not collect, use, or disclose personal information specified in this Schedule without the Ministry's written authorization.

Data is disclosed by the sender under Section 33.2 (l) of the BC *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165 ("FIPPA");

Data is collected by the receiver under Section 26 (c) and 26 (e) of FIPPA.

The parties each have authority to use the data under Section 32 (c) of FIPPA.

The parties also have authority to use the PharmaNet data under Section 22 (2) (h) of the *Pharmaceutical Services Act*.

IHA and the Ministry are governed by the provisions of FIPPA and other relevant legislation and regulation; each is responsible for ensuring FIPPA is complied with in respect of information that is collected, used or disclosed as defined by the FIPPA.

5. Physical Security of the Data

The IHA will ensure, and cause its analysts to ensure, that reasonable security arrangements are made to protect against unauthorized access, collection, use, disclosure or disposal of the data, as required under section 30 of FIPPA, including but not limited to ensuring that all data will be kept in a physically secure location and that the data will be stored in a secured database on a secured server with access being granted to only those who require it to perform their duties in connection with the Project.

The IHA will perform regular annual or more frequent information security and awareness training for all individuals with access to data. The IHA will use secure data handling procedures for electronic/hardcopy media. The IHA will have strict security provisions in place including technical, logical, personnel, and physical controls, including, but not limited

to using a Swipe Card Door Access Control System, security camera at building entrances, keys, locks, tokens, security zones, access logs, and lockable storage areas.

6. Records of Access

The IHA will maintain a record of the name of each employee or consultant who has access to the data.

The IHA will record the names of individuals, including senior information technology staff that will have access to audit records and will provide the records of access and/or audit logs to the Ministry upon request.

7. Retention of Data and Length of Data Sharing Agreement

The retention period of the Data is **two years maximum, expiring [enter date]**. The Schedule will be in force until **[enter date – same as above]**.

Upon termination of this Agreement, all data provided to the IHA must be returned to the Ministry or destroyed using a secure destruction method. If data is destroyed, the IHA will use a standard equal to or exceeding the BC government standard data destruction methods including incinerating, pulverizing or grinding the information bearing surface, cutting CD/DVD media with scissors and placing them in a locked secure shred bin for shredding by a government authorized destruction firm. If other forms of electronic media also use this data, the media will be secured prior to destruction and destroyed using one of the three BC government secure shred drop-off locations (see <http://pss.gov.bc.ca/air/media-destruction-general-public.html>).

8. Audit

The Ministry shall have the right to audit the premises and records of the IHA that are directly related to the IHA's responsibilities under this Schedule. This includes, but is not limited to the right to inspect the maintenance of records of access, the security of the data and the specific uses that have been made of the data. The IHA agrees to cooperate in this audit.

9. Reports and Publications

Neither the IHA nor its Authorized Personnel who have obtained Data may disclose Personal Information or other information that in any way could be used to identify the individuals to whom it relates, in a form which may identify those individuals.

Data are released under this Schedule to support ongoing services of the Province. These services include, but are not limited to, the production of internal reports for the purpose of program evaluation of the PHSA and/or the health authorities.

All publications, reports or presentations results must have minimum cell size of 5, and must be at LHA level or higher.

Data is not released for the purpose of marketable or media reports, but may be used for the purposes of academic journal publication provided the IHA agrees to submit complete copies of all materials intended for publication in any form to the Ministry Data Steward for approval. This advance review is required for ALL materials set for publication that rely on

the data released under this Schedule. Written approval or rejection will be provided to the IHA within 45 days of receiving the complete publication draft.

The IHA agrees to comply with this advance review.

10. Data Stewards

[name, *Title of Data Steward (i.e. CEO)*, is the signing authority for the VIHA

Shirley Wong, A/Executive Director, Information Management and Knowledge Services is the signing authority for the Ministry of Health.

11. Signatures

[name, title of data steward– *same as above*, IHA]

Date

Shirley Wong, A/Executive Director, IMKS, Ministry of Health

Date

12. Ministry Data Fields – *(insert an itemized list or table)*

*Data fields should be listed under separate database headings (MSP, DAD, etc.)
ICD 9 and ICD 10 codes should be provided when necessary (i.e. diagnostic codes)*

13. The (IHA's) Data Fields – *(insert an itemized list or table)*

14. Linkage Strategy, if applicable



MINISTRY OF HEALTH
DATA EXTRACT SCHEDULE TO DATA ACCESS
AGREEMENT

DATA ACCESS AGREEMENT NO: 2011_XX
ORGANIZATION NUMBER: 1766

Title:

Background

The [Health Authority [i.e. Fraser Health Authority; hereafter, "FHA"]] has requested access to [Medical Service Plan (MSP), Discharge Abstract Database (DAD), etc.] records for [insert region] (the "Data").

*This section identifies the context/***importance** *of the analysis and provides a brief background for the types of data requested, for example: This program was created as an initiative of this organization to evaluate health outcomes related to this chronic condition which affects several individuals annually.*

If conducting a program evaluation, name and describe the program.

Purpose:

NOTE: The purpose must identify an objective clearly related to the data request (i.e. assessment of a surveillance method, specific program evaluation, etc.) A request for data "in support of decision-making and service planning" will not suffice.

1. Specific Request for Data Access

This Schedule to the Agreement (the "Schedule") between the FHA and the BC Ministry of Health (the "Ministry"), dated January 30, 2003, with extensions, sets out specific terms for the FHA to access [MSP, DAD, etc.] for the years [enter specific date range].

FHA must not use Data disclosed under this Schedule to identify or contact any individual.

If the data request involves a specific study population (i.e. a cohort), please describe.

2. Methods of Access

- a) The data sender will provide the data receiver with either a password protected CD, or transfer the data files using a secure method such as the Secure File Delivery System or Secure File Transport Protocol that contains the data elements specified in Section 12 of this Schedule. All outgoing CD's will be password encrypted and a two-step process (one envelope containing the CD and the next letter or e-mail containing the password - If a password is send on a CD, the CD is sent separately in a sealed envelope using Rush and Trace). Software required to enable encryption such as Win Zip Self Extractor should be used with a minimum of 256 bit encryption using Advanced Encryption Standard; randomly generated minimum 64 digit password using a

combination of at least one uppercase, one lower case, and one number and may contain symbols.

- b) Passwords (if applicable) will be provided under separate cover and preferably by separate methods.

3. Data to be Disclosed

The FHA is requesting [*one-time*] access to de-identified, record-level [DAD, MSP, etc] data for the above purpose. The specific data elements requested are included in Section 12 of this Schedule.

The FHA is requesting data from [date range] (*state either calendar or fiscal year*)

[name, position, FHA], is the individual responsible for receiving the Data.
[name, position, FHA], of individuals accessing the Data.

4. Use of Data

FHA is permitted to use these data for the Purpose indicated above only.

FHA must not collect, use, or disclose personal information specified in this Schedule without the Ministry's written authorization.

Data is disclosed by the sender under Section 33.2 (l) of the BC *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165 ("FIPPA");

Data is collected by the receiver under Section 26 (c) and 26 (e) of FIPPA.

The parties each have authority to use the data under Section 32 (c) of FIPPA.

The parties also have authority to use the PharmaNet data under Section 22 (2) (h) of the *Pharmaceutical Services Act*.

FHA and the Ministry are governed by the provisions of FIPPA and other relevant legislation and regulation; each is responsible for ensuring FIPPA is complied with in respect of information that is collected, used or disclosed as defined by the FIPPA.

5. Physical Security of the Data

The FHA will ensure, and cause its analysts to ensure, that reasonable security arrangements are made to protect against unauthorized access, collection, use, disclosure or disposal of the data, as required under section 30 of FIPPA, including but not limited to ensuring that all data will be kept in a physically secure location and that the data will be stored in a secured database on a secured server with access being granted to only those who require it to perform their duties in connection with the Project.

The FHA will perform regular annual or more frequent information security and awareness training for all individuals with access to data. The FHA will use secure data handling procedures for electronic/hardcopy media. The FHA will have strict security provisions in place including technical, logical, personnel, and physical controls, including, but not limited to using a Swipe Card Door Access Control System, security camera at building entrances, keys, locks, tokens, security zones, access logs, and lockable storage areas.

6. Records of Access

The FHA will maintain a record of the name of each employee or consultant who has access to the data.

The FHA will record the names of individuals, including senior information technology staff that will have access to audit records and will provide the records of access and/or audit logs to the Ministry upon request.

7. Retention of Data and Length of Data Sharing Agreement

The retention period of the Data is **two years maximum, expiring [enter date]**. The Schedule will be in force until **[enter date – same as above]**.

Upon termination of this Agreement, all data provided to the FHA must be returned to the Ministry or destroyed using a secure destruction method. If data is destroyed, the IHA will use a standard equal to or exceeding the BC government standard data destruction methods including incinerating, pulverizing or grinding the information bearing surface, cutting CD/DVD media with scissors and placing them in a locked secure shred bin for shredding by a government authorized destruction firm. If other forms of electronic media also use this data, the media will be secured prior to destruction and destroyed using one of the three BC government secure shred drop-off locations (see <http://pss.gov.bc.ca/air/media-destruction-general-public.html>).

8. Audit

The Ministry shall have the right to audit the premises and records of the FHA that are directly related to the FHA's responsibilities under this Schedule. This includes, but is not limited to the right to inspect the maintenance of records of access, the security of the data and the specific uses that have been made of the data. The FHA agrees to cooperate in this audit.

9. Reports and Publications

Neither the FHA nor its Authorized Personnel who have obtained Data may disclose Personal Information or other information that in any way could be used to identify the individuals to whom it relates, in a form which may identify those individuals.

Data are released under this Schedule to support ongoing services of the Province. These services include, but are not limited to, the production of internal reports for the purpose of program evaluation of the PHSA and/or the health authorities.

All publications, reports or presentations results must have minimum cell size of 5, and must be at LHA lever or higher.

Data is not released for the purpose of marketable or media reports, but may be used for the purposes of academic journal publication provided the FHA agrees to submit complete copies of all materials intended for publication in any form to the Ministry Data Steward for approval. This advance review is required for ALL materials set for publication that rely on the data released under this Schedule. Written approval or rejection will be provided to the FHA within 45 days of receiving the complete publication draft.

The FHA agrees to comply with this advance review.

10. Data Stewards

[name, *Title of Data Steward (i.e. CEO)*, is the signing authority for the FHA

Shirley Wong, A/Executive Director, Information Management and Knowledge Services is the signing authority for the Ministry of Health.

11. Signatures

[name, title of data steward– *same as above*, FHA]

Date

Shirley Wong, A/Executive Director, IMKS, Ministry of Health

Date

12. Ministry Data Fields – (*insert an itemized list or table*)

Data fields should be listed under separate database headings (MSP, DAD, etc.)

ICD 9 and ICD 10 codes should be provided when necessary (i.e. diagnostic codes)

13. The (FHA's) Data Fields – (*insert an itemized list or table*)

14. Linkage Strategy, if applicable



MINISTRY OF HEALTH
DATA EXTRACT SCHEDULE TO DATA ACCESS
AGREEMENT

DATA ACCESS AGREEMENT NO: 2011_XX
ORGANIZATION NUMBER: 1762

Title:

Background

The [Health Authority [i.e. Northern Health Authority; hereafter, "NHA"]] has requested access to [Medical Service Plan (MSP), Discharge Abstract Database (DAD), etc.] records for [insert region] (the "Data").

*This section identifies the context/***importance** *of the analysis and provides a brief background for the types of data requested, for example: This program was created as an initiative of this organization to evaluate health outcomes related to this chronic condition which affects several individuals annually.*

If conducting a program evaluation, name and describe the program.

Purpose:

NOTE: The purpose must identify an objective clearly related to the data request (i.e. assessment of a surveillance method, specific program evaluation, etc.) A request for data "in support of decision-making and service planning" will not suffice.

1. Specific Request for Data Access

This Schedule to the Agreement (the "Schedule") between the NHA and the BC Ministry of Health (the "Ministry"), dated February 14, 2003, with extensions, sets out specific terms for the NHA to access [MSP, DAD, etc.] for the years [enter specific date range].

NHA must not use Data disclosed under this Schedule to identify or contact any individual.

If the data request involves a specific study population (i.e. a cohort), please describe.

2. Methods of Access

- a) The data sender will provide the data receiver with either a password protected CD, or transfer the data files using a secure method such as the Secure File Delivery System or Secure File Transport Protocol that contains the data elements specified in Section 12 of this Schedule. All outgoing CD's will be password encrypted and a two-step process (one envelope containing the CD and the next letter or e-mail containing the password - If a password is send on a CD, the CD is sent separately in a sealed envelope using Rush and Trace). Software required to enable encryption such as Win Zip Self Extractor should be used with a minimum of 256 bit encryption using Advanced Encryption Standard; randomly generated minimum 64 digit password using a

combination of at least one uppercase, one lower case, and one number and may contain symbols.

- b) Passwords (if applicable) will be provided under separate cover and preferably by separate methods.

3. Data to be Disclosed

The NHA is requesting [*one-time*] access to de-identified, record-level [DAD, MSP, etc] data for the above purpose. The specific data elements requested are included in Section 12 of this Schedule.

The NHA is requesting data from [date range] (*state either calendar or fiscal year*)

[name, position, NHA], is the individual responsible for receiving the Data.

[name, position, NHA], of individuals accessing the Data

4. Use of Data

NHA is permitted to use these data for the Purpose indicated above only.

NHA must not collect, use, or disclose personal information specified in this Schedule without the Ministry's written authorization.

Data is disclosed by the sender under Section 33.2 (c) and (l) of the BC *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165 ("FIPPA");

Data is collected by the receiver under Section 26 (c) and 26 (e) of FIPPA.

The parties each have authority to use the data under Section 32 (c) of FIPPA.

The parties also have authority to use the PharmaNet data under Section 22 (2) (h) of the *Pharmaceutical Services Act*.

NHA and the Ministry are governed by the provisions of FIPPA and other relevant legislation and regulation; each is responsible for ensuring FIPPA is complied with in respect of information that is collected, used or disclosed as defined by the FIPPA.

5. Physical Security of the Data

The NHA will ensure, and cause its analysts to ensure, that reasonable security arrangements are made to protect against unauthorized access, collection, use, disclosure or disposal of the data, as required under section 30 of FIPPA, including but not limited to ensuring that all data will be kept in a physically secure location and that the data will be stored in a secured database on a secured server with access being granted to only those who require it to perform their duties in connection with the Project.

The NHA will perform regular annual or more frequent information security and awareness training for all individuals with access to data. The NHA will use secure data handling procedures for electronic/hardcopy media. The NHA will have strict security provisions in place including technical, logical, personnel, and physical controls, including, but not limited to using a Swipe Card Door Access Control System, security camera at building entrances, keys, locks, tokens, security zones, access logs, and lockable storage areas.

6. Records of Access

The NHA will maintain a record of the name of each employee or consultant who has access to the data.

The NHA will record the names of individuals, including senior information technology staff that will have access to audit records and will provide the records of access and/or audit logs to the Ministry upon request.

7. Retention of Data and Length of Data Sharing Agreement

The retention period of the Data is **two years maximum, expiring [enter date]**. The Schedule will be in force until **[enter date – same as above]**.

Upon termination of this Agreement, all data provided to the FHA must be returned to the Ministry or destroyed using a secure destruction method. If data is destroyed, the IHA will use a standard equal to or exceeding the BC government standard data destruction methods including incinerating, pulverizing or grinding the information bearing surface, cutting CD/DVD media with scissors and placing them in a locked secure shred bin for shredding by a government authorized destruction firm. If other forms of electronic media also use this data, the media will be secured prior to destruction and destroyed using one of the three BC government secure shred drop-off locations (see <http://pss.gov.bc.ca/air/media-destruction-general-public.html>).

8. Audit

The Ministry shall have the right to audit the premises and records of the NHA that are directly related to the NHA's responsibilities under this Schedule. This includes, but is not limited to the right to inspect the maintenance of records of access, the security of the data and the specific uses that have been made of the data. The NHA agrees to cooperate in this audit.

9. Reports and Publications

Neither the NHA nor its Authorized Personnel who have obtained Data may disclose Personal Information or other information that in any way could be used to identify the individuals to whom it relates, in a form which may identify those individuals.

Data are released under this Schedule to support ongoing services of the Province. These services include, but are not limited to, the production of internal reports for the purpose of program evaluation of the PHSA and/or the health authorities.

All publications, reports or presentations results must have minimum cell size of 5, and must be at LHA lever or higher.

Data is not released for the purpose of marketable or media reports, but may be used for the purposes of academic journal publication provided the NHA agrees to submit complete copies of all materials intended for publication in any form to the Ministry Data Steward for approval. This advance review is required for ALL materials set for publication that rely on the data released under this Schedule. Written approval or rejection will be provided to the NHA within 45 days of receiving the complete publication draft.

The NHA agrees to comply with this advance review.

10. Data Stewards

[name, *Title of Data Steward (i.e. CEO)*, is the signing authority for the FHA

Shirley Wong, is the Ministry of Health A/Chief Data Steward.

11. Signatures

[name, title of data steward– *same as above*, NHA]

Date

Shirley Wong, A/Chief Data Steward, Ministry of Health

Date

12. Ministry Data Fields – (*insert an itemized list or table*)

Data fields should be listed under separate database headings (MSP, DAD, etc.)

ICD 9 and ICD 10 codes should be provided when necessary (i.e. diagnostic codes)

13. The (NHA's) Data Fields – (*insert an itemized list or table*)

14. Linkage Strategy, if applicable



MINISTRY OF HEALTH
DATA EXTRACT SCHEDULE TO DATA ACCESS
AGREEMENT

DATA ACCESS AGREEMENT NO: 2012_XXXX
ORGANIZATION NUMBER: 1767

Title:

Background

The Provincial Health Services ("PHSA") has requested access to [Medical Service Plan ("MSP"), Discharge Abstract Database ("DAD"), PharmaNet ("PNET"), etc.] records for [insert region and date range] (the "Data").

*This section identifies the context/***importance** *of the analysis and provides a brief background for the types of data requested, for example: This program was created as an initiative of this organization to evaluate health outcomes related to this chronic condition which affects several individuals annually.*

If conducting a program evaluation, name and describe the program.

Purpose:

NOTE: The purpose must identify an objective clearly related to the data request (i.e. assessment of a surveillance method, specific program evaluation, etc.) A request for data "in support of decision-making and service planning" will not suffice.

1. Specific Request for Data Access

This Schedule to the Agreement (the "Schedule") between the PHSA and the BC Ministry of Health (the "Ministry"), dated February 12, 2003, with extensions, sets out specific terms for the PHSA to access [MSP, DAD, PNET, etc.] for the years [enter specific date range].

The PHSA must not use Data disclosed under this Schedule to identify or contact any individual.

If the data request involves a specific study population (i.e. a cohort), please describe.

2. Methods of Access

- a) The data sender will provide the data receiver with either a password protected CD, or transfer the data files using a secure method such as the Secure File Delivery System or Secure File Transport Protocol that contains the data elements specified in Section 12 of this Schedule. All outgoing CD's will be password encrypted and a two-step process (one envelope containing the CD and the next letter or e-mail containing the password - If a password is sent on a CD, the CD is sent separately in a sealed envelope using Rush and Trace). Software required to enable encryption such as Win Zip Self Extractor should be used with a minimum of 256 bit encryption using Advanced Encryption Standard; randomly generated minimum 64 digit password using a

combination of at least one uppercase, one lower case, and one number and may contain symbols.

- b) Passwords (if applicable) will be provided under separate cover and preferably by separate methods.

3. Data to be Disclosed

The PHSA is requesting [*one-time*] access to de-identified, record-level [*DAD, MSP, PNET, etc*] data for the above purpose. The specific data elements requested are included in Section 12 of this Schedule.

The PHSA is requesting data from [*date range*] (*state either calendar or fiscal year*)

[*name, position, PHSA*], is the individual responsible for receiving the Data.

[*name, position, PHSA*], of individuals accessing the Data.

4. Use of Data

The PHSA is permitted to use these data for the purpose indicated above only.

The PHSA must not collect, use, or disclose personal information specified in this Schedule without the Ministry's written authorization.

Data are disclosed by the sender under Section 33.2 (c) and (l) of the BC *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165 ("FIPPA").

Data are collected by the receiver under Section 26 (c) and 26 (e) of FIPPA.

The parties each have authority to use the data under Section 32 (c) of FIPPA.

The parties also have authority to use the PharmaNet data under Section 22 (2) (h) of the *Pharmaceutical Services Act*.

The PHSA and the Ministry are governed by the provisions of FIPPA and other relevant health legislation and regulation(s); each is responsible for ensuring FIPPA is complied with in respect of information that is collected, used or disclosed as defined by the FIPPA.

5. Physical Security of the Data

The PHSA will ensure, and cause its analysts to ensure, that reasonable security arrangements are made to protect against unauthorized access, collection, use, disclosure or disposal of the data, as required under section 30 of FIPPA, including but not limited to ensuring that all data will be kept in a physically secure location and that the data will be stored in a secured database on a secured server with access being granted to only those who require it to perform their duties in connection with the project.

The PHSA will perform regular annual or more frequent information security and awareness training for all individuals with access to Data. The PHSA will use secure data handling procedures for electronic/hardcopy media. The PHSA will have strict security provisions in place including technical, logical, personnel, and physical controls, including, but not limited to using a Swipe Card Door Access Control System, security camera at building entrances, keys, locks, tokens, security zones, access logs, and lockable storage areas.

6. Records of Access

The PHSA will maintain a record of the name of each employee or consultant who has access to the Data.

The PHSA will record the names of individuals, including senior information technology staff that will have access to audit records and will provide the records of access and/or audit logs to the Ministry upon request.

7. Retention of Data and Length of Data Sharing Agreement

The retention period of the Data is **two years maximum, expiring [enter date]**. The Schedule will be in force until **[enter date – same as above]**.

Upon termination of this Agreement, all Data provided to the PHSA must be returned to the Ministry or destroyed using a secure destruction method. If data is destroyed, the PHSA will use a standard equal to or exceeding the BC government standard data destruction methods including incinerating, pulverizing or grinding the information bearing surface, cutting CD/DVD media with scissors and placing them in a locked secure shred bin for shredding by a government authorized destruction firm. If other forms of electronic media also use this data, the media will be secured prior to destruction and destroyed using one of the three BC government secure shred drop-off locations (see <http://pss.gov.bc.ca/air/media-destruction-general-public.html>).

8. Audit

The Ministry shall have the right to audit the premises and records of the PHSA that are directly related to the PHSA's responsibilities under this Schedule. This includes, but is not limited to the right to inspect the maintenance of records of access, the security of the Data and the specific uses that have been made of the Data. The PHSA agrees to cooperate in this audit.

9. Reports and Publications

Neither the PHSA nor its Authorized Personnel who have obtained Data may disclose Personal Information or other information that in any way could be used to identify the individuals to whom it relates, in a form which may identify those individuals.

Data are released under this Schedule to support ongoing services of the Province. These services include, but are not limited to, the production of internal reports for the purpose of program evaluation of the PHSA and/or the health authorities.

All publications, reports or presentations results must have minimum cell size of 5, and must be at LHA lever or higher.

Data is not released for the purpose of marketable or media reports, but may be used for the purposes of academic journal publication. The PHSA agrees to submit complete copies of all materials intended for publication in any form to the Ministry Data Steward for approval. This advance review is required for ALL materials set for publication that rely on the data released under this Schedule. Written approval or rejection will be provided to the PHSA within 45 days of receiving the complete publication draft.

The PHSA agrees to comply with this advance review.

10. Data Stewards

[name, *Title of Data Steward (i.e. President)*, is the signing authority for the PHSA].

Shirley Wong, is the Ministry of Health A/Chief Data Steward.

11. Signatures

[name, title of Data Steward– *same as above*, The PHSA]

Date

Shirley Wong, A/Chief Data Steward, Ministry of Health

Date

12. Ministry Data Fields – (*insert an itemized list or table*)

Data fields should be listed under separate database headings (MSP, DAD, etc.)

ICD 9 and ICD 10 codes should be provided when necessary (i.e. diagnostic codes)

13. The PHSA Data Fields - (*insert an itemized list or table*)

14. Linkage Strategy, if applicable



MINISTRY OF HEALTH
DATA EXTRACT SCHEDULE TO DATA ACCESS
AGREEMENT

DATA ACCESS AGREEMENT NO: 2011_XX
ORGANIZATION NUMBER: 1765

Title:

Background

The [Health Authority [i.e. Vancouver Coastal Health Authority; hereafter, "VCHA"]] has requested access to [Medical Service Plan (MSP), Discharge Abstract Database (DAD), etc.] records for [insert region] (the "Data").

*This section identifies the context/***importance** *of the analysis and provides a brief background for the types of data requested, for example: This program was created as an initiative of this organization to evaluate health outcomes related to this chronic condition which affects several individuals annually.*

If conducting a program evaluation, name and describe the program.

Purpose:

NOTE: The purpose must identify an objective clearly related to the data request (i.e. assessment of a surveillance method, specific program evaluation, etc.) A request for data "in support of decision-making and service planning" will not suffice.

1. Specific Request for Data Access

This Schedule to the Agreement (the "Schedule") between the VCHA and the BC Ministry of Health (the "Ministry"), dated January 14, 2003, with extensions, sets out specific terms for the VCHA to access [MSP, DAD, etc.] for the years [enter specific date range].

VCHA must not use Data disclosed under this Schedule to identify or contact any individual.

If the data request involves a specific study population (i.e. a cohort), please describe.

2. Methods of Access

- a) The data sender will provide the data receiver with either a password protected CD, or transfer the data files using a secure method such as the Secure File Delivery System or Secure File Transport Protocol that contains the data elements specified in Section 12 of this Schedule. All outgoing CD's will be password encrypted and a two-step process (one envelope containing the CD and the next letter or e-mail containing the password - If a password is send on a CD, the CD is sent separately in a sealed envelope using Rush and Trace). Software required to enable encryption such as Win Zip Self Extractor should be used with a minimum of 256 bit encryption using Advanced Encryption Standard; randomly generated minimum 64 digit password using a

combination of at least one uppercase, one lower case, and one number and may contain symbols.

- b) Passwords (if applicable) will be provided under separate cover and preferably by separate methods.

3. Data to be Disclosed

The VCHA is requesting [*one-time*] access to de-identified, record-level [DAD, MSP, etc] data for the above purpose. The specific data elements requested are included in Section 12 of this Schedule.

The VCHA is requesting data from [date range] (*state either calendar or fiscal year*)

[name, position, VCHA], is the individual responsible for receiving the Data.
[name, position, VCHA], of individuals accessing the Data

4. Use of Data

VCHA is permitted to use these data for the Purpose indicated above only.

VCHA must not collect, use, or disclose personal information specified in this Schedule without the Ministry's written authorization.

Data is disclosed by the sender under Section 33.2 (l) of the BC *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165 ("FIPPA");

Data is collected by the receiver under Section 26 (c) and 26 (e) of FIPPA.

The parties each have authority to use the data under Section 32 (c) of FIPPA.

The parties also have authority to use the PharmaNet data under Section 22 (2) (h) of the *Pharmaceutical Services Act*.

VCHA and the Ministry are governed by the provisions of FIPPA and other relevant legislation and regulation; each is responsible for ensuring FIPPA is complied with in respect of information that is collected, used or disclosed as defined by the FIPPA.

5. Physical Security of the Data

The VCHA will ensure, and cause its analysts to ensure, that reasonable security arrangements are made to protect against unauthorized access, collection, use, disclosure or disposal of the data, as required under section 30 of FIPPA, including but not limited to ensuring that all data will be kept in a physically secure location and that the data will be stored in a secured database on a secured server with access being granted to only those who require it to perform their duties in connection with the Project.

The VCHA will perform regular annual or more frequent information security and awareness training for all individuals with access to data. The VCHA will use secure data handling procedures for electronic/hardcopy media. The VCHA will have strict security provisions in place including technical, logical, personnel, and physical controls, including, but not limited to using a Swipe Card Door Access Control System, security camera at building entrances, keys, locks, tokens, security zones, access logs, and lockable storage areas.

6. Records of Access

The VCHA will maintain a record of the name of each employee or consultant who has access to the data.

The VCHA will record the names of individuals, including senior information technology staff that will have access to audit records and will provide the records of access and/or audit logs to the Ministry upon request.

7. Retention of Data and Length of Data Sharing Agreement

The retention period of the Data is **two years maximum, expiring [enter date]**. The Schedule will be in force until **[enter date – same as above]**.

Upon termination of this Agreement, all data provided to the [HA] must be returned to the Ministry or destroyed using a secure destruction method. If data is destroyed, the [HA] will use a standard equal to or exceeding the BC government standard data destruction methods including incinerating, pulverizing or grinding the information bearing surface, cutting CD/DVD media with scissors and placing them in a locked secure shred bin for shredding by a government authorized destruction firm. If other forms of electronic media also use this data, the media will be secured prior to destruction and destroyed using one of the three BC government secure shred drop-off locations (see <http://pss.gov.bc.ca/air/media-destruction-general-public.html>).

8. Audit

The Ministry shall have the right to audit the premises and records of the VCHA that are directly related to the VCHA's responsibilities under this Schedule. This includes, but is not limited to the right to inspect the maintenance of records of access, the security of the data and the specific uses that have been made of the data. The VCHA agrees to cooperate in this audit.

9. Reports and Publications

Neither the VCHA nor its Authorized Personnel who have obtained Data may disclose Personal Information or other information that in any way could be used to identify the individuals to whom it relates, in a form which may identify those individuals.

Data are released under this Schedule to support ongoing services of the Province. These services include, but are not limited to, the production of internal reports for the purpose of program evaluation of the PHSA and/or the health authorities.

All publications, reports or presentations results must have minimum cell size of 5, and must be at LHA lever or higher.

Data is not released for the purpose of marketable or media reports, but may be used for the purposes of academic journal publication provided the VCHA agrees to submit complete copies of all materials intended for publication in any form to the Ministry Data Steward for approval. This advance review is required for ALL materials set for publication that rely on the data released under this Schedule. Written approval or rejection will be provided to the VCHA within 45 days of receiving the complete publication draft.

The VCHA agrees to comply with this advance review.

10. Data Stewards

[name, *Title of Data Steward (i.e. CEO)*, is the signing authority for the VCHA.

Shirley Wong, A/Executive Director, Information Management and Knowledge Services is the signing authority for the Ministry of Health.

11. Signatures

[name, title of data steward– *same as above*, VCHA]

Date

Shirley Wong, A/Executive Director, IMKS, Ministry of Health

Date

12. Ministry Data Fields – (*insert an itemized list or table*)

Data fields should be listed under separate database headings (MSP, DAD, etc.)

ICD 9 and ICD 10 codes should be provided when necessary (i.e. diagnostic codes)

13. The (VCHA) Data Fields – (*insert an itemized list or table*)

14. Linkage Strategy, if applicable



MINISTRY OF HEALTH
DATA EXTRACT SCHEDULE TO DATA ACCESS
AGREEMENT

DATA ACCESS AGREEMENT NO: 2011_XX
ORGANIZATION NUMBER: 1764

Title:

Background

The [Health Authority [i.e. Vancouver Island Health Authority; hereafter, "VIHA"]] has requested access to [Medical Service Plan (MSP), Discharge Abstract Database (DAD), etc.] records for [insert region] (the "Data").

This section identifies the context/importance of the analysis and provides a brief background for the types of data requested, for example: This program was created as an initiative of this organization to evaluate health outcomes related to this chronic condition which affects several individuals annually.

If conducting a program evaluation, name and describe the program.

Purpose:

NOTE: The purpose must identify an objective clearly related to the data request (i.e. assessment of a surveillance method, specific program evaluation, etc.) A request for data "in support of decision-making and service planning" will not suffice.

1. Specific Request for Data Access

This Schedule to the Agreement (the "Schedule") between the VIHA and the BC Ministry of Health (the "Ministry"), dated February 3, 2003, with extensions, sets out specific terms for the VIHA to access [MSP, DAD, etc.] for the years [enter specific date range].

VIHA must not use Data disclosed under this Schedule to identify or contact any individual.

If the data request involves a specific study population (i.e. a cohort), please describe.

2. Methods of Access

- a) The data sender will provide the data receiver with either a password protected CD, or transfer the data files using a secure method such as the Secure File Delivery System or Secure File Transport Protocol that contains the data elements specified in Section 12 of this Schedule. All outgoing CD's will be password encrypted and a two-step process (one envelope containing the CD and the next letter or e-mail containing the password - If a password is send on a CD, the CD is sent separately in a sealed envelope using Rush and Trace). Software required to enable encryption such as Win Zip Self Extractor should be used with a minimum of 256 bit encryption using Advanced Encryption Standard; randomly generated minimum 64 digit password using a

combination of at least one uppercase, one lower case, and one number and may contain symbols.

- b) Passwords (if applicable) will be provided under separate cover and preferably by separate methods.

3. Data to be Disclosed

The VIHA is requesting [*one-time*] access to de-identified, record-level [DAD, MSP, etc] data for the above purpose. The specific data elements requested are included in Section 12 of this Schedule.

The VIHA is requesting data from [date range] (*state either calendar or fiscal year*)

[name, position, VIHA], is the individual responsible for receiving the Data.

[name, position, VIHA], of individuals accessing the Data

4. Use of Data

VIHA is permitted to use these data for the Purpose indicated above only.

VIHA must not collect, use, or disclose personal information specified in this Schedule without the Ministry's written authorization.

Data is disclosed by the sender under Section 33.2 (l) of the BC *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165 ("FIPPA");

Data is collected by the receiver under Section 26 (c) and 26 (e) of FIPPA.

The parties each have authority to use the data under Section 32 (c) of FIPPA.

The parties also have authority to use the PharmaNet data under Section 22 (2) (h) of the *Pharmaceutical Services Act*.

VIHA and the Ministry are governed by the provisions of FIPPA and other relevant legislation and regulation; each is responsible for ensuring FIPPA is complied with in respect of information that is collected, used or disclosed as defined by the FIPPA.

5. Physical Security of the Data

The VIHA will ensure, and cause its analysts to ensure, that reasonable security arrangements are made to protect against unauthorized access, collection, use, disclosure or disposal of the data, as required under section 30 of FIPPA, including but not limited to ensuring that all data will be kept in a physically secure location and that the data will be stored in a secured database on a secured server with access being granted to only those who require it to perform their duties in connection with the Project.

The VIHA will perform regular annual or more frequent information security and awareness training for all individuals with access to data. The VIHA will use secure data handling procedures for electronic/hardcopy media. The VIHA will have strict security provisions in place including technical, logical, personnel, and physical controls, including, but not limited to using a Swipe Card Door Access Control System, security camera at building entrances, keys, locks, tokens, security zones, access logs, and lockable storage areas.

6. Records of Access

The VIHA will maintain a record of the name of each employee or consultant who has access to the data.

The VIHA will record the names of individuals, including senior information technology staff that will have access to audit records and will provide the records of access and/or audit logs to the Ministry upon request.

7. Retention of Data and Length of Data Sharing Agreement

The retention period of the Data is **two years maximum, expiring [enter date]**. The Schedule will be in force until **[enter date – same as above]**.

Upon termination of this Agreement, all data provided to the VIHA must be returned to the Ministry or destroyed using a secure destruction method. If data is destroyed, the VIHA will use a standard equal to or exceeding the BC government standard data destruction methods including incinerating, pulverizing or grinding the information bearing surface, cutting CD/DVD media with scissors and placing them in a locked secure shred bin for shredding by a government authorized destruction firm. If other forms of electronic media also use this data, the media will be secured prior to destruction and destroyed using one of the three BC government secure shred drop-off locations (see <http://pss.gov.bc.ca/air/media-destruction-general-public.html>).

8. Audit

The Ministry shall have the right to audit the premises and records of the VIHA that are directly related to the VIHA's responsibilities under this Schedule. This includes, but is not limited to the right to inspect the maintenance of records of access, the security of the data and the specific uses that have been made of the data. The VIHA agrees to cooperate in this audit.

9. Reports and Publications

Neither the VIHA nor its Authorized Personnel who have obtained Data may disclose Personal Information or other information that in any way could be used to identify the individuals to whom it relates, in a form which may identify those individuals.

Data are released under this Schedule to support ongoing services of the Province. These services include, but are not limited to, the production of internal reports for the purpose of program evaluation of the PHSA and/or the health authorities.

All publications, reports or presentations results must have minimum cell size of 5, and must be at LHA lever or higher.

Data is not released for the purpose of marketable or media reports, but may be used for the purposes of academic journal publication provided the VIHA agrees to submit complete copies of all materials intended for publication in any form to the Ministry Data Steward for approval. This advance review is required for ALL materials set for publication that rely on the data released under this Schedule. Written approval or rejection will be provided to the VIHA within 45 days of receiving the complete publication draft.

The VIHA agrees to comply with this advance review.

10. Data Stewards

[name, *Title of Data Steward (i.e. CEO)*, is the signing authority for the VIHA

Shirley Wong, A/Executive Director, Information Management and Knowledge Services is the signing authority for the Ministry of Health.

11. Signatures

[name, title of data steward– *same as above*, VIHA]

Date

Shirley Wong, A/Executive Director, IMKS, Ministry of Health

Date

12. Ministry Data Fields – (*insert an itemized list or table*)

Data fields should be listed under separate database headings (MSP, DAD, etc.)

ICD 9 and ICD 10 codes should be provided when necessary (i.e. diagnostic codes)

13. The (VIHA's) Data Fields – (*insert an itemized list or table*)

14. Linkage Strategy, if applicable

8 High Risk information Sharing Situations

HSIMT has identified eight high risk information sharing situations related to PSD and FCSD.

HSIMT reviewed those information sharing situations with the program areas and based on the information provided downgraded them as follow:

MOH and Canada Border Service Agency (FCSD)

IMKS reviewed this information sharing situation with Monica Uribe, Manager, Eligibility, Compliance and Enforcement. It was determined that under the current process clients provide signed consents to the Ministry to request crossing information from Canada Boarder Service Agency. It was also determined that in the future the “read only” access to CBSA crossing database would be granted to someone holding a Peace Officer Status and when that happens ISA will be signed. Given that the information is currently being shared with informed consent from clients, the applicable risk-level is being downgraded from high to **MEDIUM**.

MOH and Third Party Insurers (FCSD)

IMKS reviewed this information sharing situation with Marie Thelisma, Director, Audit and Investigation Branch. It was determined that all communications with certain insurers were done on an ad-hoc basis in the course of regular audit business of practitioners. The request letters were sent to the third party stating legislation requirement to provide the information needed and documentation required for the audit. All requests are always done by letter. Template letter was provided. As this information sharing is done through request letters for the purpose of audit, this information sharing situation is downgraded to **LOW**.

MOH and Patients and/or physicians (FCSD)

IMKS reviewed this information sharing situation with Rita King, Manager, Pharmacare Audit. It was determined that the practice of sending letters to the doctors through confirmation process was discontinued. Letters to confirm pharmacy billings to PharmaCare were sent only to patients. Patients would receive letters with a random selection of medications that a particular pharmacy has billed using their PHN. The only information sharing situation was with the client, and the ministry confirmed their information. The random patient confirmation letter program is part of operational procedures. This information sharing situation was downgraded to **LOW**.

MOH and Ministry of Finance/Revenue Solutions Branch (FCSD)

IMKS reviewed this information sharing situation with Darlene Ell, Director, Decision Support. It was determined that an Information Sharing Agreement between the MOH and MOF (Revenue Solutions) covers the Monthly Deductible Payment Option Program. Under the agreement, information is disclosed by MOH to MOF, and the MOF discloses personal information to MOH as Health determines an individual's eligibility for *MDPO* and MOF is responsible for administering the MDPO account. MOH and MOF are currently updating this ISA. This information Sharing situation was downgraded to **LOW**.

MOH and the College of Pharmacists of BC (PSD)

IMKS reviewed this information sharing situation with Liz Keay, Policy Analyst, Policy Outcomes, Evaluation and Research Branch and later confirmed with Mitch Moneo, A/ Executive Director, Policy Outcomes Evaluation and Research. It was determined that the College of Pharmacists has a TUA with the Ministry/ PSD to provide personal profiles for clients. The College of Pharmacists has direct access to PNet as service provider. Also, the ministry has no access to the client's PNet data. As there is an existing TUA, this information sharing situation was downgraded to **MEDIUM**.

MOH and Medication Management Canada (PSD)

IMKS reviewed this information sharing situation with Liz Keay, Policy Analyst, Policy Outcomes, Evaluation and Research Branch and later confirmed with Mitch Moneo, A/ Executive Director, Policy Outcomes Evaluation and Research. It was determined that this project is on hold. This information sharing situation was downgraded to **LOW**.

MOH and contract Physicians (PSD)

IMKS reviewed this information sharing situation with Liz Keay, Policy Analyst, Policy Outcomes, Evaluation and Research Branch and later confirmed with Mitch Moneo, A/ Executive Director, Policy Outcomes Evaluation and Research. It was determined that physicians are under contract with the ministry. As physicians are under contract with the ministry, this information sharing situation was downgraded to **LOW**.

MOH and prescribers (physicians and nurse practitioners) (PSD)

IMKS reviewed this information sharing situation with Liz Keay, Policy Analyst, Policy Outcomes, Evaluation and Research Branch and later confirmed with Mitch Moneo, A/ Executive Director, Policy Outcomes Evaluation and Research. It was determined that adjudication of Special Authority requests are done either by ministry's employees or ministry contractors. As adjudications were done by employees or contractors, this information sharing situation was downgraded to **LOW**.

Medium and Low Risk Information Sharing Situations by the Program Areas

MEDIUM RISK	
Program Area	Number of Information Sharing Situations
Pharmaceutical Services Division (PSD)	6
Financial and Corporate Services Division (FCSD)	3
LOW RISK	
Program Area	Number of Information Sharing Situations
Vital Statistics Agency (VSA)	40
Pharmaceutical Services Division (PSD)	6
Financial and Corporate Services Division (FCSD)	6
Health Link BC	5
Office of the Provincial Health Officer (PHO)	2
Medical Services/Human Health Resources (MSHHRD)	1
OUT OF SCOPE/NOT APPLICABLE	37
TOTAL	106

Risk Measure

Third-Party Information Sharing Situations

NON-Agreement Situations - Active at March 31, 2013

High Risk Category

- Personally identifiable information (PII) – includes only:
 - Personal Health Number (PHN)
 - Name (first, middle, last – or any combination)
- Data sharing situation also involves:
 - PII is being exchanged as of March 31, 2013 – and needs to continue

6.3 - MITIGATION STRATEGY – Produce ISAs for situations that meet above criteria

Medium Risk Category

- PII includes:
 - Full Date of Birth
 - Full Date of Death
 - 6-digit postal code
- De-identified record-level information (e.g. identifiers replaced with Study ID)

6.3 - MITIGATION STRATEGY – Document number of situations, propose longer-term plan

Low Risk Category

- Aggregated information with small cell sizes
- Potential for individual identification exists, but probability is low
- Contractors with business contact information

6.3 - MITIGATION STRATEGY – Document number of situations, propose longer-term plan

6.2 – Risk Measure - KEY ASSUMPTIONS

1. Legislative authority exists for each in-scope data sharing situation; otherwise, situation may be halted and sent to AG for review at program area's expense;
2. 'Personally identifiable information' includes PHN and/or Name - and does not include full date of birth, death, or 6-digit postal code - unless attached to either PHN or Name.
3. Application of the 6.3 Risk Measure is not precedent setting, is independent of any corporate governance model, and must not be used to guide data sharing situations outside of 6.3.

	Risk Categorization		
	High	Medium	Low
Third-party data sharing as of March 31, 2013 NOTE: Does not include health authority data sharing			
Personally Identifiable Information (PII) <ul style="list-style-type: none"> Personal Health Number (PHN) NAME (First and/ Middle, Last) 	✓		
Personally Identifiable Information (PII) <ul style="list-style-type: none"> Full Date of Birth Full Date of Death Postal Code 		✓	
De-identified record-level information		✓	
Aggregated Information (cell size >5)			✓

ROADMAP

Medium and Low Risk Information Sharing Situations

MEDIUM RISK INFORMATION SHARING SITUATIONS (9)

- Identify program areas involved
- Send e-mails to executives advising that IMKS need to evaluate this situations and asking for assistance
- Conduct one-on-one meeting with the program area
- Review information sharing situation and identify harm
- Determine what steps are needed to mitigate situations
- Close file

LOW RISK INFORMATION SHARING SITUATIONS (60)

Review information sharing situations with Vital Statistics Agency (40)

- Send e-mails to executives advising that IMKS need to evaluate this situations and asking for assistance
- Conduct one-on-one meeting with VSA
- Review information sharing situations and identify harm
- Determine when information sharing situations are operational procedures that require or do not require ISA
- Determine what steps are needed to mitigate situations
- Close file

Review remaining low risk information sharing situations (20)

- Identify program areas involved
- Send e-mails to executives advising that IMKS need to evaluate this situations and asking for assistance
- Conduct one-on-one meeting with the program area
- Review information sharing situation and identify harm
- Determine when information sharing situations are operational procedures that require or do not require ISA
- Identify information sharing situations that covered by GSA, and when expire, if necessary, renew them using new template
- Determine what steps are needed to mitigate situations
- Close file

PARALLEL PROCESSES/PRIORITIES

- Identify ISA that do not have expiration date
- Identify program areas with those ISAs
- Introduce 3 years maximum term to all amendments

Canadian Payments Practice Experience Survey

Name	
Level	
Office	
Service Line	

Instructions:

Please review the list of clients and knowledge areas below, and mark an "X" in the appropriate boxes

1. Participation

I would like to be identified as a Canadian payments practitioner	
I am not interested in participating in this practice (skip survey)	

Leader: I am the primary Deloitte contact for payments work at this client

Team: I have payments delivery experience at this client (via Deloitte or previous employer)

Contacts: No delivery experience, but I have contacts in the organization's payments group

2. Client Coverage (Payments experience only. If you are a company alum please add a note)

2a. Large Financial Institutions	Leader	Team	Contacts	Notes
BMO				
CIBC				
Desjardins				
Laurentian				
National				
RBC				
Scotia				
TD				
Other International (List)				
2b. Small FI/Monolines	Leader	Team	Contacts	Notes
ATB				
Canadian Tire Financial				
Capital One				
Central 1				
CUCC				
JP Morgan Chase				
Other CU or CU Central (list)				
PC Financial				
P&W Bank				
Rogers Bank				
Vancity				
Other (List)				
2c. Payments Networks	Leader	Team	Contacts	Notes
American Express				
Exchange Network				
Interac/Acsys				
MasterCard				
PayPal				
Visa				
2d. Acquirers/Processors	Leader	Team	Contacts	Notes
Celero Systems				
Chase Paymentech				
Everlink				
First Data				
Global Payments				
Intria				

Moneris				
PSiGate				
Symcor				
TD Merchant Services				
Threshold				
VersaPay				
Other (list)				
2e. Other Players	Leader	Team	Contacts	Notes
CPA				
Other Forex (list)				
Payday/Cheque Cashing (list)				
Payments Task Force				
PRESTO				
RC Mint				
Western Union				
Other (List)				

3. International Payments Experience (via Deloitte or previous employer)		
Jurisdiction	I have delivered work here	Notes
US		
UK		
Europe (list)		
Middle East (list)		
Africa (list)		
China		
India		
Australia		
Other Asia/Pacific (list)		
LACRO (list)		

Expert: I could serve as a SME on a client engagement

Skilled: I could be sold as an experienced practitioner on a client engagement

Basic: I am familiar with high-level concepts and issues in this area

4. Functional Capabilities				
Skill Area	Expert	Skilled	Basic	Notes
Acquiring/POS				
AML				
ATM Technology				
Authentication				
B2B/Commercial Payments				
Bill Pay				
Card Portfolio M&A				
Cheques/Paper				
Collections				
Contact Centres				
Credit Cards				
Debit Cards				
Disbursements				
eInvoicing & Payments				
EMV Technology				
eWallets				
FDR Implementation				
Forex				
Fraud/Risk				
Mobile Payments				
Money Transfer				

Online Payments				
Platform Implementation				
Prepaid				
Private/White Label				
Regulations				
Retail Acceptance				
Rewards				
Security/PCI				
SWIFT				
Transaction Processing				
Transit Payments				
Treasury				
TSYS Implementation				
Wholesale Payments				
Other (List)				

5. Other	
I don't have specific experience but would like to work in payments	
I'm in DMS and would like to support the Payments COE	

6. Additional Comments	

External Service Providers List

1. In Scope

The scope of the project includes logging for:

Service Provider	Systems	Contract Contact
	s.15	Andrew Elderfield

2. Out of Scope

Service Provider	Systems	Rationale
		Robust logging enabled
		Robust logging enabled
	s.15	O/S logging to be considered in project 7.2
		Network logging and log correlation options to be considered in project 7.2

Pages 503 through 507 redacted for the following reasons:

s. 15

s. 15, s.22


Summary Table

Quick Estimate Summary	
Service Request Estimate Title	Implementation of Basic Audit logging on databases with Personally Identifiable Information (PII)
CAST #	9944
Reference	
Requestor	Rhys Smallwood : (250) 952-2457 Rhys.Smallwood@gov.bc.ca
Date Requested	2013/09/19
Application	
Priority	High
Base/Non-Base	Pool

Revision Log

Date	Version	Summary of change(s)	Changes marked
Sep 19, 2013	V 0.1	Initial version	
Sep 20, 2013	V 0.2	Extend list of applications based on feedback regarding DB platforms	

Related Documentation

File	File Name
 2013-09-18 - CGI Supported Applications	2013-09-18 - CGI Supported Applications - Application Database PI Confirmation - Master copy.xlsx

1 Overview

This estimate provides the amount of effort required to implement basic database audit procedures on several applications identified by Deloitte and the Ministry of Health as Personal Identifiable Information holders.

This initiative intends to record all activity on the data sources for these applications to provide a tool to identify any attempt to access or obtain information through the application, the database server or any other possible connection to the data sources.

2 Assumptions

The following assumptions have determined the scope of this estimate:

s.15

3 Estimate

Quick Estimate ¹		
Task	Comments/Special Considerations/Task/Estimate Assumptions	Effort Estimate (Hours)
Analysis/Design	Determine data sources to be audited and technique to implement auditing procedures	8
Documentation	Detailed log of activities completed	4
Implementation	1 hr per database x 15 databases	15
Acceptance Testing (UAT)	Determine results meet business requirements 1 hour per database (SQL Server, Oracle DBs)	15
Quality Assurance	Verify results and usability of results 1 hr per database (TO BE DETERMINED)	15
Project Management	Project Management, communications and Meetings	12
Other	Contingency	6
Total Effort		75

¹ Note: A reasonable effort has been expended in determining the above "Quick Estimate" based on knowledge of the application and the requirements received at the time the estimate was prepared. As CGI has not completed detailed investigation and analysis in completing this "Quick Estimate", CGI cannot be bound to this estimate.

Pages 510 through 515 redacted for the following reasons:

- s. 15
- s. 15, s.22
- s.15



Purpose: Identify Ministry sources and source logs required to realize each Threat Category

Source Type #	In Scope Sources	Managed by: (MoH, SSBC, HPAS, CGI, Other)	Responsible Person	Description of Business Application	Platform information	OS information	Application information	Estimated EPS
------------------	------------------	---	-----------------------	--	----------------------	----------------	-------------------------	------------------

Pages 517 through 519 redacted for the following reasons:

s. 15



	Database	Application	Desktop	Unsure
COO				
Finance - Accounting Operations				
Finance - Audit & Investigations				
Health Authorities Division				

s. 15

Database	Application	Desktop	Unsure
HealthLink BC			
Vital Statistics			
PHO <i>(Stores Copies only)</i>			
Planning & Innovation 1			
Planning & Innovation 2		\$ 15	
Population & Public Health - N McGuire			
PSD 1			
PSD 2			

P8.2 information
security program roles
and responsibilities
BC Ministry of Health



September 5, 2013

Table of contents

- Introduction
- Assessment results
- Recommendations
- Roadmap

Introduction



Objectives

Enhancement opportunities

- There is an opportunity to enhance clarity of roles, responsibilities and accountability with respect to the MOH security program.

Initiative objectives

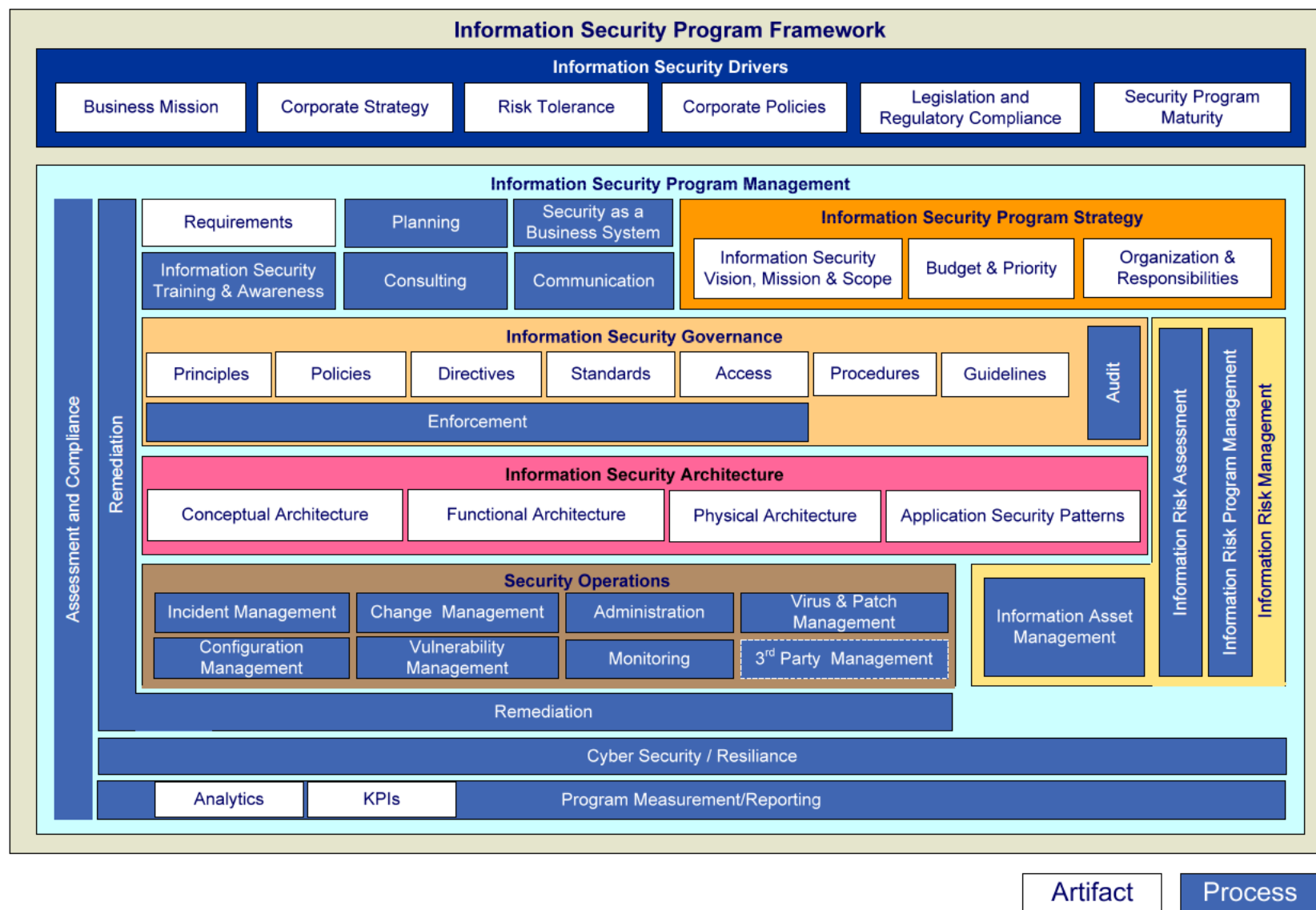
1. Understand what information security processes and operations the current MOH security specific employees and service providers are undertaking
2. Map the current processes and operations to an industry Information Security Framework
3. Identify gaps and provide recommendations for improvement where applicable

Interviewees

Six senior members of management in information security, management and technology were interviewed as part of the assessment:

- Deb McGinnis, Executive Director, Health Information Privacy, Security and Legislation Branch (HIPSL), Victoria
- Ken Madden, Director HIPSL, Information Security and Audit, Victoria
- Shirley Wong, Director, Information Management and Knowledge Services (IMKS), Victoria
- Darcy Goodwin, Executive Director, Corporate Management & Operations, Victoria
- Don Stewart, Director, Corporate Management & Operations, Systems Services, Victoria
- Suzanne Jennings, A/Director, BC Vital Stats, Information Technology Services, Victoria

Information security program framework



Assessment results

Scope & effectiveness rating scale

The following ratings have been applied to the roles and responsibilities assessment in the following section.

Scope		
1	2	3
Not in place within MoH	Operating at Divisional level	Operating at Ministry level

Effectiveness		
1	2	3
Not effective	Limited effectiveness	Operating effectively *

* This engagement was based on interviews and therefore effectiveness is based on responses from interviews and has not been validated through testing.

Pages 530 through 532 redacted for the following reasons:

s.15

Recommendations

Risk ratings for recommendations

The following ratings have been applied to the recommendations in the following section.

Rating	Risk
H (High)	The weakness is critical to overall information security, or the risk (combination of likelihood and consequence) is high and will effect the integrity, confidentiality and availability of systems for a large group of users.
M (Medium)	The weakness is important to information security but not critical to everyone. The risk is medium (combination of likelihood and consequence) and the integrity, availability and confidentiality of selected users would be impacted.
L (Low)	The weakness is relevant, but not critical or there is an estimated limited chance that the risk will occur. The risk is low (combination of likelihood and consequence) and the integrity, availability and confidentiality of selected users can be impacted.

Pages 535 through 541 redacted for the following reasons:

s.15

Security Program – Operating Model Options

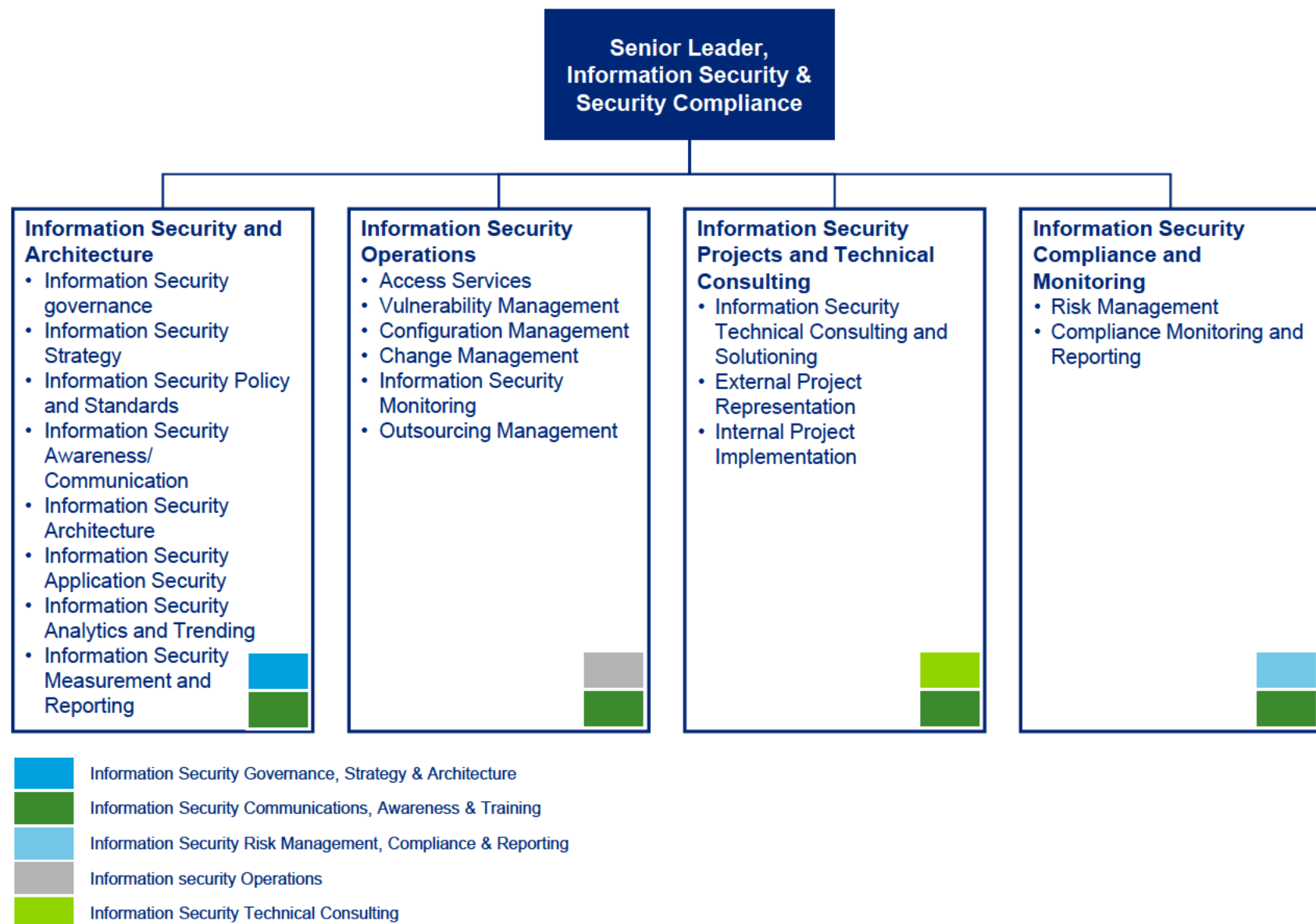
Current key security individuals

Branch	Selected key security individuals	Stated security focus
HIPSL	Deb McGinnis, Executive Director	Overall IT Security Strategy, Policies, Procedures, Interfacing with OCIO Privacy including compliance activities and advisory support as the privacy officer Training & Awareness
	Heather Dunlop, Director	Privacy including compliance activities Legislation
	Ken Madden, Director	IT Security Policies, Procedures, Strategy Interfacing with OCIO Information Security Auditing and Compliance Audit framework and management manual Security Threat Risk Assessments Logging and Monitoring capabilities Training & Awareness
	Gwen Lock, Manager	Interface with various other divisions within MOH Information Security Advisory Support Various scanning activities
IMKS	Shirley Wong, Director	Executive and advisory support for IT Governance Access management for data warehouses Configuration management for data warehouses Physical security for data warehouses
	Stephen Braniff, Director	Configuration management Vulnerability and patch management Architecture
	Martin Townson, Manager	Access control for IMKS controlled data

Current key security individuals (cont.)

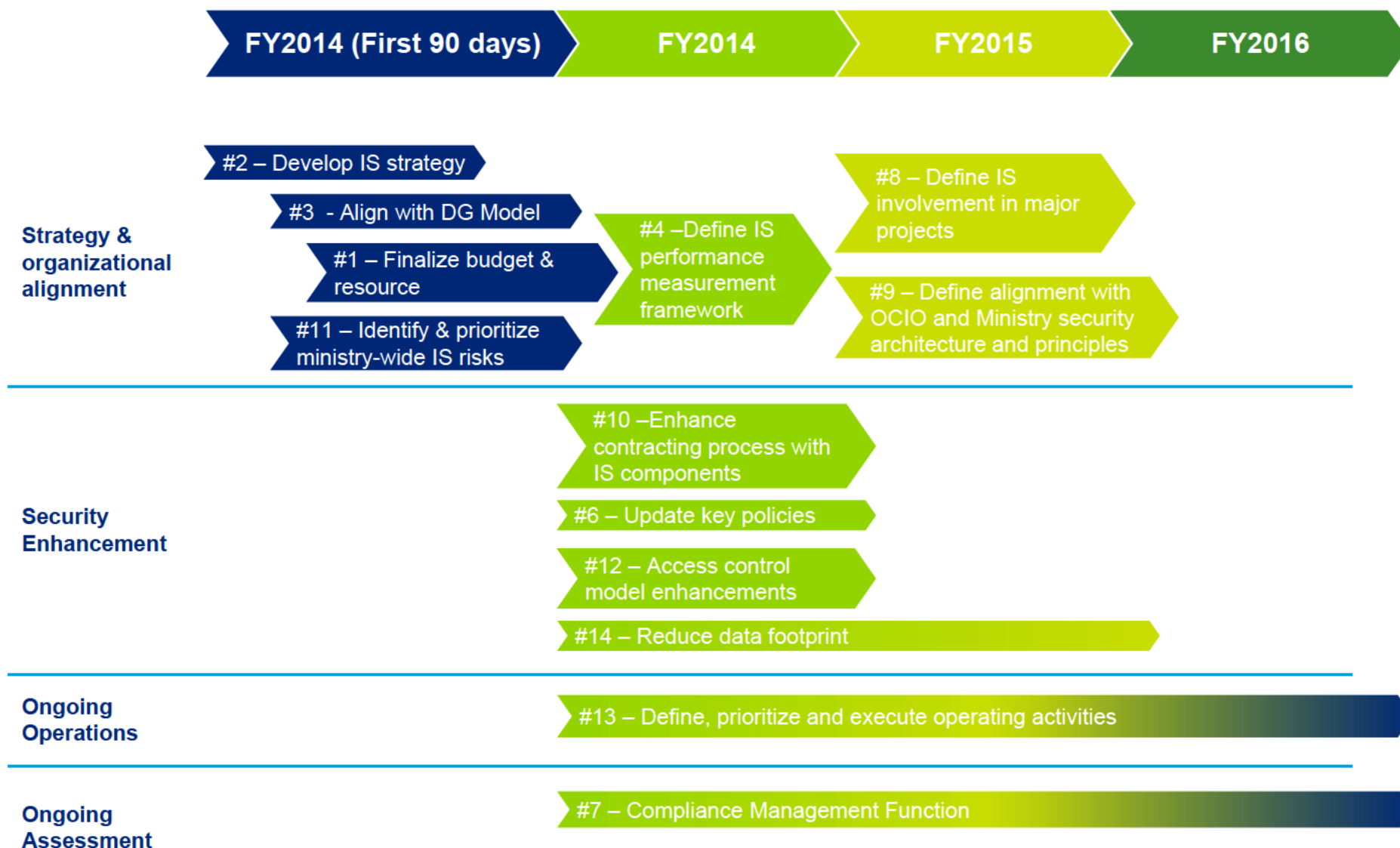
Branch	Selected Key Security Individuals	Stated Security Focus
BC Vital Stats	Suzanne Jennings, A/Director	Access control to BC Vital Stats data
	Yanni Vasilakopoulos, Database Administrator	Access control specific to database Performance based KPIs Configuration Management, Vulnerability Management
Corporate Management & Operations	Darcy Goodwin, Executive Director	Interfacing with OCIO Portfolio of applications management Policy exemption requests (typically with respect to Vulnerability management) IT Contract management Incident Response
	Don Stewart, Director	IT Contract management Security Architecture Procurement initiatives

Desired security state



Roadmap

Roadmap



Immediate next steps

Before any action is to be taken on the various recommendations for improvement, Deloitte suggest the following immediate next steps.

1. Establish an agreement at the executive level of the scope of what needs to be done and obtain approval for the 3 year plan outlined in this document.
2. Formalize the mandate and budget for the plan.
3. Formalize the roles and responsible within the security group and dedicate those resources to the plan.

Appendix

High-level organizational roles

High-level framework for discussion (PDCA)

	Information Security	Information Privacy
Plan	<ul style="list-style-type: none"> • Business objectives • Security strategy 	<ul style="list-style-type: none"> • Business objectives • Privacy strategy
Do	<ul style="list-style-type: none"> • Develop policies & procedures • Allocate resources • Education • Security Operations • Security Administration • Advisory services 	<ul style="list-style-type: none"> • Develop policies & procedures • Allocate resources • Education • Privacy operations • Advisory Services • Legislation – interpretation
Check	<ul style="list-style-type: none"> • Monitoring • Reporting • Follow up assessments 	<ul style="list-style-type: none"> • Monitoring • Reporting • Follow up assessments
Act	<ul style="list-style-type: none"> • Enhancement • Remediation 	<ul style="list-style-type: none"> • Enhancement • Remediation

High-level overview of select activities/processes

Security Privacy	HIPSL	IMKS	CM&O	Vital Statistics	Strategic Projects	Service providers
Plan	<ul style="list-style-type: none"> Objectives & Strategy (Sector-wide) 	<ul style="list-style-type: none"> Operations planning Operations budget mgmt. 	<ul style="list-style-type: none"> IT Strategy Planning IT Budget mgmt. 	-	-	<ul style="list-style-type: none"> Strategy Budget mgmt.
Do	<ul style="list-style-type: none"> Policies Procedures Security & Privacy advisory services Interpretation Incident response Risk register 	<ul style="list-style-type: none"> Policies Procedures Logging Access control 	<ul style="list-style-type: none"> Contract mgmt. Incident Response 	<ul style="list-style-type: none"> Access control Config & vulnerability mgmt. 	-	<ul style="list-style-type: none"> Policies Procedures Logging & monitoring Access control Patch mgmt.
Check	<ul style="list-style-type: none"> STRAs PIAs Compliance assessments 	<ul style="list-style-type: none"> Access reviews Log reviews 	-	-	-	<ul style="list-style-type: none"> Audits (external) Reporting
Act	<ul style="list-style-type: none"> Security & Privacy advisory services Interpretation 	<ul style="list-style-type: none"> Security architecture Design Implement 	<ul style="list-style-type: none"> Security architecture 	-	<ul style="list-style-type: none"> Security Architecture Design Implement 	<ul style="list-style-type: none"> Design Implement Operate Access control

Current challenges and open questions

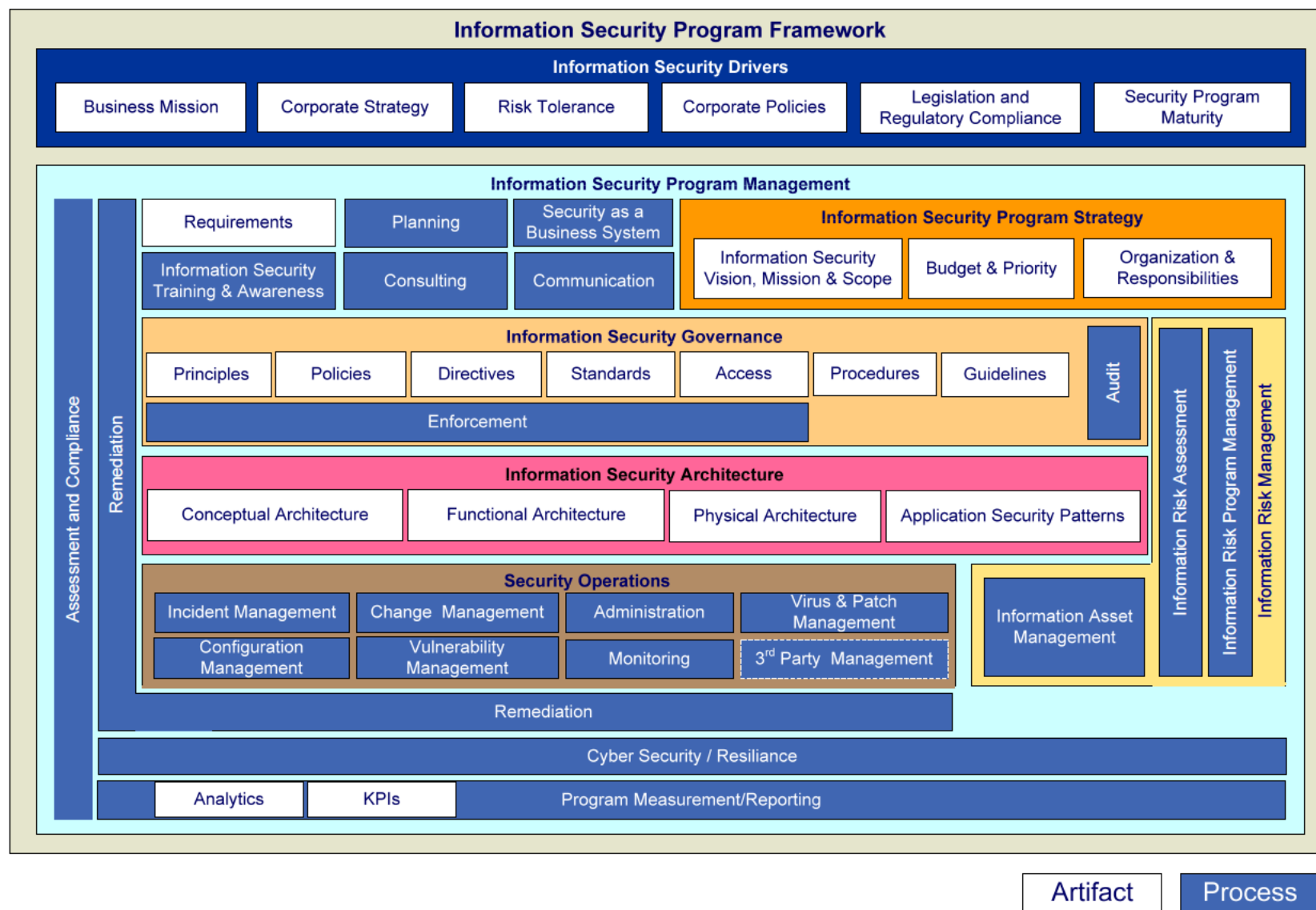
- Plan
 - There is an opportunity to improve alignment between the Ministry's IT and IT Security planning processes
 - This will facilitate the development of a Ministry Security Strategy
 - This strategy provides the opportunity to define a security vision and plan for the Ministry that is:
 - Comprehensive while being pragmatic (addressing policy and regulatory requirements where possible,
 - Relevant
 - Based on

Overview of information security program framework

Information security program framework

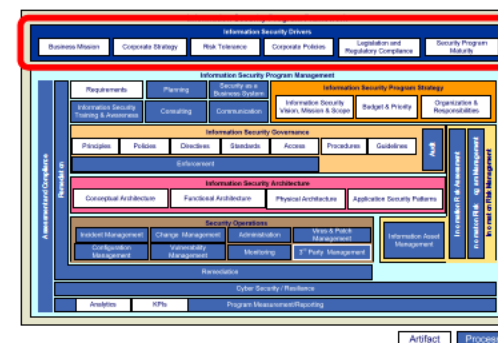
- **Information Security Program Management** including management and the definition of information protection and security requirements, planning, training and awareness, enterprise-wide communications, assessment and compliance and measurement and reporting of the Information Protection and Security Program.
- **Information Security Program Strategy** including the definition and maintenance of the vision, mission, scope and organization roles and responsibilities
- **Information Security Governance** including information protection and security governance framework, the information security policy, standards process development and maintenance, the information security measurement and reporting program and the assurance and compliance criteria and reporting requirements.
- **Information Security Architecture** including responsibility for the architecture layers and liaison with the other parts of the organization.
- **Information Risk Management** including the executive incident response process, risk assessments, information asset management and risk management methodology development.
- **Information Security Operations** including information security vulnerability management and event monitoring, incident response coordination, change management, configuration management, management of outsourcing arrangements and the administrative support necessary to perform user account management. This also includes the security operation of the business and support applications.

Information security program framework



Information security drivers

- **Business Mission:** The main purpose of the organization – why does the organization exist? What does it strive to accomplish?
- **Corporate Strategy:** The collection of beliefs and behaviours that provide the operational compass for the organization.
- **Risk Tolerance:** Represents the determined level of risk that is acceptable to the organization.
- **Corporate Policies:** The statements of responsibilities and obligation that defines the way the organization will operate in business.
- **Legislation and Regulatory Compliance:** The collection of legislation and regulations that the corporation is subject to that include requirements directed at the information security program.
- **Security Program Maturity:** A relative index, level or determination of the maturity of the current information security program.



Information security program management

- **Requirements:** The collection of requirements that defines the basis for the information security program and the initiatives for continuous improvement.

ISO References: A6.2.2 Addressing security when dealing with customers

A12.1.1 Security requirements analysis and specification

- **Planning:** Represents the ongoing process of assessing the state of operation of the information security program and defining activities and initiatives to be applied for continuous improvement.

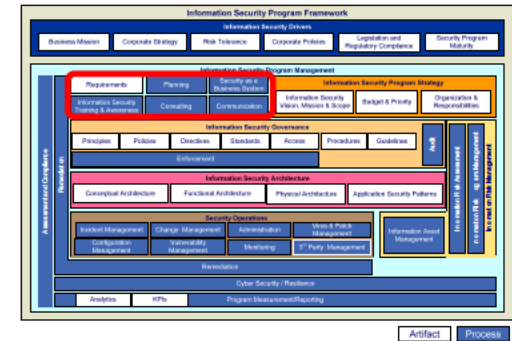
ISO References: A10.3.1 Capacity management

- **Security as a Business System:** The ongoing process of supporting organization portfolio management or business decisions from components of the information security program. Also includes the processes for supporting the ongoing operation of the information security program as a corporate business system following the Plan-Do-Check-Act model and processes for continuous improvement.

ISO References: 4.2.1 Establish the ISMS

- **Information Security Training & Awareness:** The ongoing process of informing the various constituencies on the information security risks and their individual responsibilities and obligations for managing the risks.

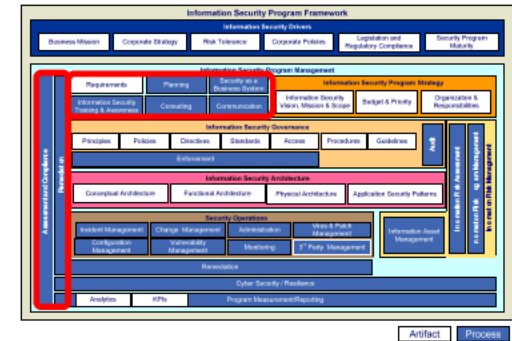
ISO References: A8.2.2 Information security awareness, education, and training



Artifact Process

Information security program management (cont'd)

- **Consulting:** The ongoing process of providing security subject matter experts to other parts of the enterprise on an as-needed or planned basis.
- **Communication:** The ongoing responsibility and process for communicating the appropriate information concerning the ongoing operation, support for and adherence to the information security program.
- **Remediation:** The process for applying controls or processes to remediate identified weaknesses in the information security program.



ISO References: 4.2.4 Maintain and improve the ISMS

- **Assessment and Compliance:** The process of examining an organization's information security program and providing recommendations for audit, and/or certification preparation.

ISO References: A6.1.8 Independent review of information security

A15.1 Compliance with legal requirements (A15.1.1, A15.1.2, A15.1.3, A15.1.4, A15.1.5, A15.1.6)

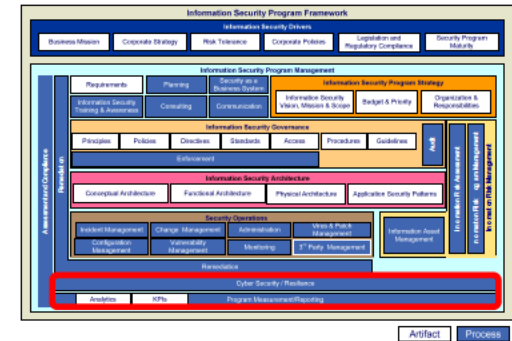
A15.2.2 Technical compliance checking

Information security program management (cont'd)

- **Cyber Security/Resilience:** Includes the process and responsibilities for planning for and dealing with cyber security threats and maintaining the information and communication processes to limit the impact in the event of cyber security threats or incidents (resilience).

ISO References:

- A6.1.6 Contact with authorities
- A6.1.7 Contact with special interest groups
- A10.10.2 Monitoring system use
- A13.1.1 Reporting information security events

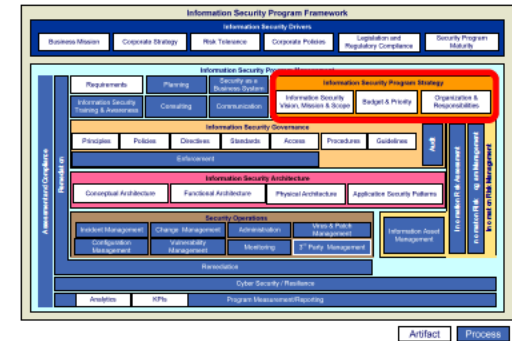


- **Program Measurement/Reporting:** Includes the components for the measurement and reporting of the effectiveness of the information security program using ongoing measurements through tools such as Key Performance Indicators (KPIs).
 - **Analytics:** The tools and processes for monitoring, defining, modeling and reacting to information risks.
 - **KPIs:** The definition and collection of Key Performance Indicators (KPIs) that are used to measure the activities and actions of the information security program.

ISO References: 4.2.3 Monitor and review the ISMS

Information security program strategy

- **Information Security Vision, Mission & Scope:** The statements of purpose and operational focus that directs the responsibilities, plans and boundaries of the Information Security Program.
- **Budget & Priority:** The processes for allocating budget and assigning priority to initiatives to continuously improve the information security program.
- **Organization & Responsibilities:** The defined organization structure and assigned responsibilities that are required to support the information security program.



ISO References: A6.1 Internal Organization (A6.1.1, A6.1.2, A6.1.3, A6.1.4, A6.1.6, A6.1.7)
A8.1 Human Resources Security (A8.1.1)

Information security governance

- **Information Security Principles:** A statement of value, operation or belief that defines the organization's approach to security. The principles define the philosophy of the organization that influence the definition of the security policies

ISO References: A10.1.3 Segregation of duties

- **Information Security Policy:** The statements of intent and guidance by senior management to the organization as a whole regarding the commitment, ownership, responsibilities, processes and other themes applicable to security

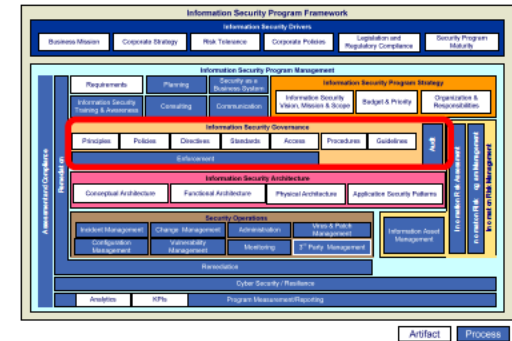
ISO References: A5.1 Information Security Policy (A5.1.1, A5.1.2)

A6.1.5 Confidentiality agreements

A7.2 Information classification (A7.2.1, A7.2.2)

- **Information Security Directives:** The documented statements of information security decisions that direct mandatory compliance to criteria essential for managing the organization's information management risk. These are many times defined as 2nd tier policies.

ISO References: A5.1 Information Security Policy (A5.1.1, A5.1.2)



Information security governance (cont'd)

- **Information Security Standards:** A requirement for compliance for a particular means of executing a security function resulting from a security policy. The security standard defines what methods and mechanisms that will be used to enforce the policy.

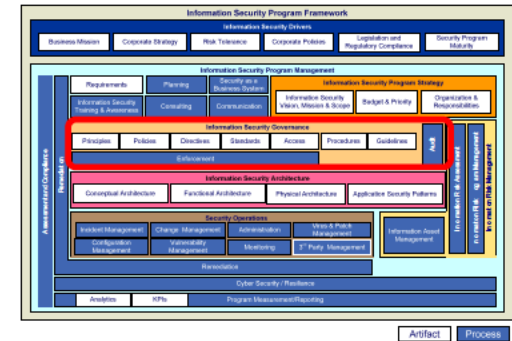
ISO References: A10.7 Media handling (A10.7.1, A10.7.2, A10.7.3, A10.7.4)
A10.8 Exchange of Information (A10.8.1, A10.8.2, A10.8.3, A10.8.4, A10.8.5)
A11.3 User responsibilities (A11.3.1, A11.3.2, A11.3.3)

- **Information Security Procedures:** Includes descriptions of the specific steps that must be followed to carry out one or more of the responsibilities defined in a security standard. The security procedure defines what steps are required to apply the security standards.

ISO References: A10.1.1 Documented operating procedures
A10.5 Back (A10.1.1)

- **Information Security Access:** The specification and processes for governance of access entitlements to information resources. Access governance provides the business decision base for enabling identity and access management systems.

ISO References: A11.1 Business requirements for access control (A11.1.1)
A11.6 Application and Information access control (A11.6.1, A11.6.2)



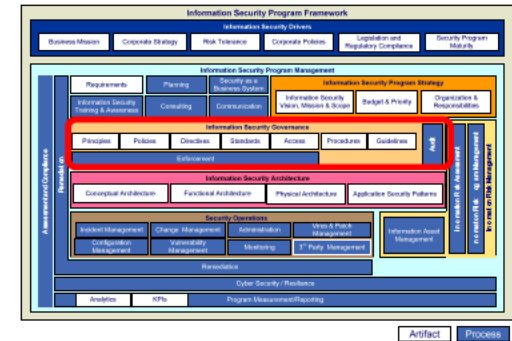
Information security governance (cont'd)

- **Information Security Guidelines:** Are the statements of advice concerning good business practice to retain a secure environment. The Information Security Guidelines describe optional and additional security measures and procedures that can be followed to enhance security.
- **Information Security Enforcement:** The ongoing actions and responsibilities for assessing compliance to the information security program, identifying areas of non-compliance and initiating actions for remediation of the non-compliance.

ISO References: A15.2 Compliance with security policies and standards, and technical compliance (A15.2.1, A15.2.2)

- **Information Security Audit:** The process of assessing compliance of the information security program to the reference standard defined by the organization's policies, standards and procedures.

ISO References: A15.3 Information systems audit considerations (A15.3.1, A15.3.2)



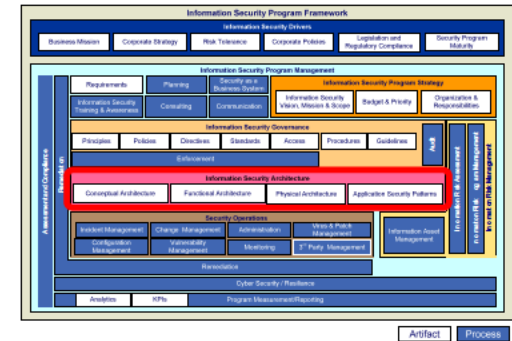
Information security architecture

- **Information Security Conceptual Architecture:** A description of the business organization and relationships sufficient to ensure all stakeholders can understand and agree with the information security principles or functions represented.

ISO References: A11.4.5 Segregation in networks
 A10.1.4 Separation of development, test and operational facilities

- **Information Security Functional Architecture:** A description of the information security building blocks defining the required information security functions, protocols and interfaces in a logical and formal manner.

ISO References: A10.6 Network security management (A10.6.1, A10.6.2)
 A10.9 Electronic commerce services (A10.9.1, A10.9.2, A10.9.3)
 A11.4 Network Access Control (A11.4.1, 11.4.2, 11.4.3, A11.4.4, A11.4.5, A11.4.6, A11.4.7)
 A11.5 Operating system access control (A11.5.1, A11.5.2, A11.5.3, A11.5.4, A11.5.5, A11.5.6)
 A11.7 Mobile computing and teleworking (A11.7.1, A11.7.2)
 A12.3 Cryptographic controls (A12.3.1, A12.3.2)
 A12.4 Security of system files (A12.4.2, A12.4.3)



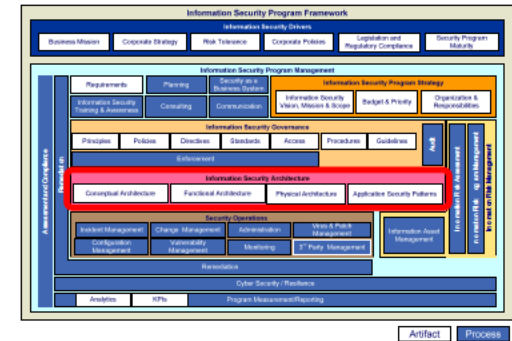
Information security architecture (cont'd)

- **Information Security Physical Architecture:** Applies the technical standards, specifications and solutions to the functional requirements identified in the Functional Architecture.

ISO References:	A10.6 Network security management (A10.6.1, A10.6.2)
	A10.9 Electronic commerce services (A10.9.1, A10.9.2, A10.9.3)
	A11.4 Network Access Control (A11.4.1, 11.4.2, 11.4.3, A11.4.4, A11.4.5, A11.4.6, A11.4.7)
	A11.5 Operating system access control (A11.5.1, A11.5.2, A11.5.3, A11.5.4, A11.5.5, A11.5.6)
	A11.7 Mobile computing and teleworking (A11.7.1, A11.7.2)
	A12.3 Cryptographic controls (A12.3.1, A12.3.2)
	A12.4 Security of system files (A12.4.2, A12.4.3)

- **Information Security Architecture Patterns:** A collection of predetermined technologies and configurations for developing applications that when followed, provide a standard base of information security.

ISO References:	A12.2 Correct processing in applications (A12.2.1, A12.2.2, A12.2.3, A12.2.4)
	A 12.5 Security in development and support processes (A12.5.1, A12.5.2, A12.5.3, A12.5.4, A12.5.5)



Information risk management

- **Information Risk Assessment:** The processes and tools used to identify the vulnerabilities and potential threats to the information assets and to assess the resulting risks to which the information assets are exposed in order to identify, select and apply the appropriate safeguards.

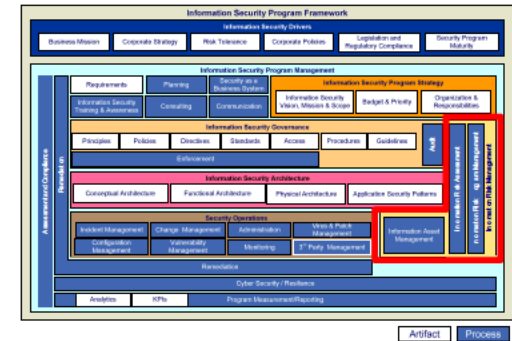
ISO References: 4.2.1 Establish the ISMS
A6.2.1 Identification of risks related to external parties
A6.2.3 Addressing security in third party agreements

- **Information Risk Program Management:** The decisions and processes required to manage the information risk management program on an ongoing basis.

ISO References: 4.2.1 Establish the ISMS
4.2.2 Implement and operate the ISMS

- **Information Asset Management:** The processes, repositories and guidance to identify, classify, value and assess information assets. An effective risk assessment process relies on understanding the assets and asset value that is being assessed for information risk.

ISO References: A7.1 Responsibility for assets (A7.1.1, A7.1.2, A7.1.3)



Information security operations

- **Incident Management:** The ongoing processes required to systematically Detect, report and manage identified information security incidents.

ISO References: A13.1 Reporting information security events and weaknesses (A13.1.1, A13.1.2)

A13.2 Management of information security incidents and improvements (A13.2.1, A13.2.2, A13.2.3)

- **Configuration Management:** The method and processes for maintaining standard configurations for technology and infrastructure to support an identified information security posture.

ISO References: A10.3.2 System Acceptance

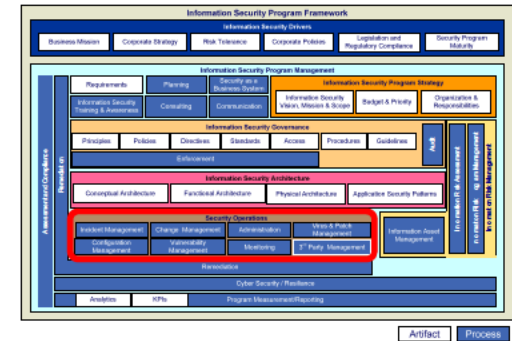
A12.4.1 Control of operational software

- **Vulnerability Management:** The ongoing processes for discovering or detecting, assessing and addressing vulnerabilities in the IT environment.

ISO References: A12.6 Technical vulnerability management (A12.6.1)

- **Monitoring:** The ongoing surveillance of the operational components and processes of the information security program and detection and notification of significant events.

ISO References: A 10.10 Monitoring (A10.10.1, A10.10.2, A10.10.3, A10.10.4, A10.10.5, A10.10.6)



Information security operations (cont'd)

- **Change Management:** The processes for effectively managing change to the information security program components.

ISO References: A10.1.2 Change management

- **3rd Party Management:** The criteria and processes for managing the information security components that are applied and managed by another party through an outsourcing or other formal agreements.

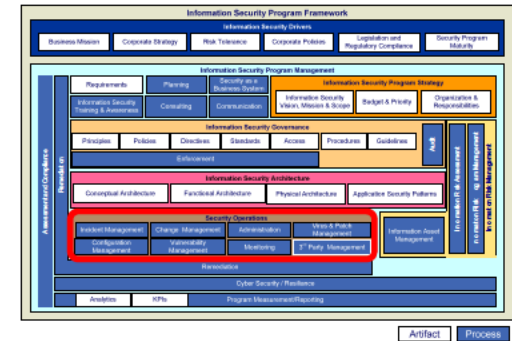
ISO References: A10.2 Third party service delivery management (A10.2.1, A10.2.2, A10.2.3)

- **Administration:** Includes the processes for effectively managing change to the Information Protection and Security Program components and the processes for administering the information security components such as identity management and network component management.

ISO References: 11.2 User Access Management (A11.2.1, A11.2.2, A11.2.3, A11.2.4)

- **Virus & Patch Management:** The ongoing processes for managing the virus protection program and the program for maintaining the current software levels of the supporting IT infrastructure.

ISO References: A10.4. Protection against malicious and mobile code (A10.4.1, A10.4.2)



Project 10.1

Compliance Management



Contents

- The role of the compliance function
- Compliance function mandate
- Governance considerations
- Implementation strategy considerations

Role of the Compliance Function

Role of the compliance function

- Compliance functions are typically designed to support adherence to external and internal policies, regulations and directives
- The following outlines the typical responsibilities of a compliance function
 - Develop a cross-organization view of compliance drivers and risks
 - Develop and implement a compliance management program, with a focus on monitoring, assessment and reporting
 - Provide subject matter expertise to the organization on compliance-related matters
 - Leverage internal and external subject matter experts in specific domains to support compliance activities
 - Regularly report results to a senior executive body
 - Monitor and report on remediation progress and results
 - Support investigations, audits or related assessments by third parties by acting as the primary point of contact and coordination

The role of the compliance function (cont'd)

- The mandate, structure, governance and operations of compliance functions vary significantly across industries (due to varying regulatory requirements)
- These functions also vary across organizations within a given industry (due to the need for an effective compliance function to be driven by organization-specific compliance requirements, risks, risk tolerance, etc.)
- Often, compliance functions are tasked with advising and monitoring the organization
- While both functions are critical, the need for objectivity and independence must be considered and addressed

Mandate

Compliance function mandate

- The mandate defines the domains for which compliance function is responsible for assessing performance and alignment to authoritative guidance (policies, regulations, directives, etc.)
- The mandate also describes the scope for which the compliance function is responsible. This includes organizational boundaries, systems, processes, etc.
- Mandates are typically informed by key compliance drivers and risks and are driven by a risk-based approach to ensure best use of limited resources
- The proposed mandate outlined below is based on identified compliance drivers and recommendations arising from recent assessment and investigation activities
- The mandate and scope of the compliance function is expected to evolve over time in response to changing risks, compliance drivers, compliance performance and incidents
- **NOTE:** The intent of the compliance function outlined in this document is to focus on information security and privacy. Other compliance domains are being considered in other parts of the Ministry, and alignment (organizationally and in terms of processes and governance) should be considered over time

MoH internal compliance drivers*

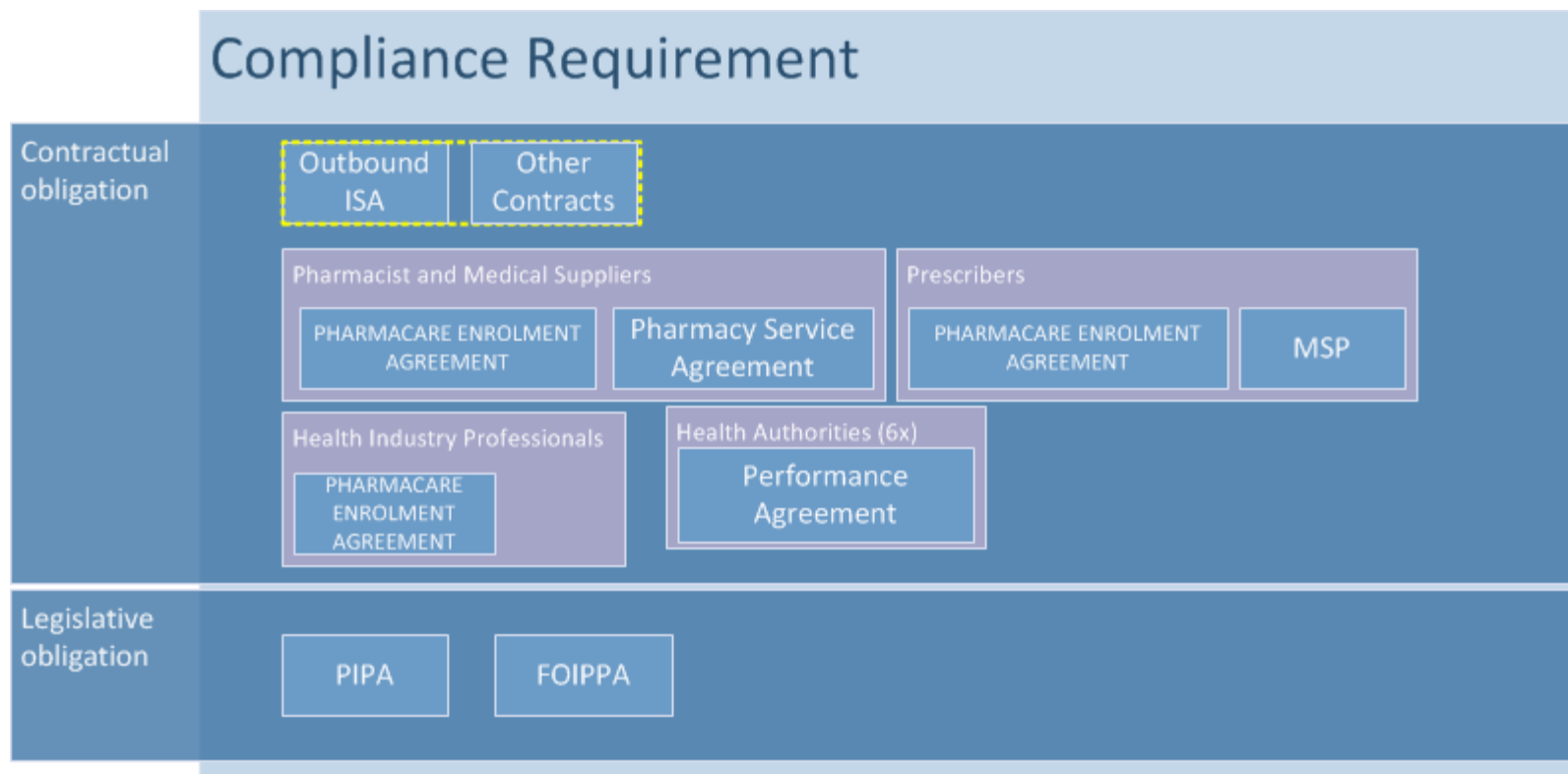
Requirement
Type

Compliance Requirement

Contractual obligation	<div>Inbound ISA</div> <div>Other Contracts</div>
Legislative obligation	<div>British Columbia Cancer Agency Research Information Regulation</div> <div>E-Health Regulation</div> <div>FOIPPA</div> <div>Ministry of Health Act</div> <div>Disclosure of Prescribed Information Regulation</div> <div>Pharmacy Operations and Drug Scheduling Act</div> <div>Dissemination of Information Regulation</div> <div>Electronic Transaction Act</div> <div>STATISTICS ACT</div> <div>VETERINARY DRUGS ACT</div> <div>Pharmaceutical Services Act</div> <div>Reciprocal Taxation Agreement Regulation</div> <div>Financial Administration Act</div>
BC Gov Core Policy	<div>Section 1 - Governance</div> <div>Section 2 - General and Financial Management</div> <div>Section 3 - Planning, Budgeting and Reporting</div> <div>Section 4 - Expense Management</div> <div>Section 5 - Capital Asset Management</div> <div>Section 6 - Procurement</div> <div>Section 7 - Revenue and Receivables Management</div> <div>Section 8 - Asset Management</div> <div>Section 9 - Guarantees and Indemnities</div> <div>Section 10 - Travel</div> <div>Section 11 - Transportation</div> <div>Section 12 - Information Management and Information Technology Management</div> <div>Section 13 - Financial Systems and Controls</div> <div>Section 14 - Risk Management</div> <div>Section 15 - Security</div> <div>Section 16 - Business Continuity Management</div> <div>Section 17 - Internal Audit</div> <div>Section 18 - Administration</div> <div>Section 19 - Corporate Compliance and Controls Monitoring</div> <div>Section 20 - Loss Management</div> <div>Section 21 - Government Transfers</div> <div>BC Info Sec Policy</div>
MoH Policy	<div>Ministry of Health Policies</div>
Rulings	<div>OIPC reports and rulings</div>

* Yellow boxes denote potential areas of focus based on recent assessments and investigations.

MoH third-party (outbound data) compliance requirements



* Yellow boxes denote potential areas of focus based on recent assessments and investigations.

Examples of recent compliance drivers (OIPC findings)¹

- Known compliance drivers for MOH:
 - OIPC observations (examples):
 - “There was **no audit** at any level of employee or researcher compliance with privacy policies”
 - “Lack of sufficient **executive commitment**...to privacy and security compliance”
 - “the resources invested in ensuring thorough privacy protection within information sharing agreements might be wasted because there is **no follow-up** to ensure researchers are complying with privacy and security requirements”
 - OIPC recommendation
 - “The Ministry executive should implement an effective program for **monitoring and auditing compliance** by **employees** with privacy controls, and by **contracted researchers** and **academic researchers** with privacy provisions in agreements, to enable proactive detection of unauthorized use and disclosure of Ministry information.”

¹ Office of the Information & Privacy Commissioner for BC. 2013. Investigation Report F13-02 – Ministry of Health.

Current Compliance Activities (Summary)

- Current understanding based on document review and discussions
 - Internal Systems Audit and Compliance Charter and Terms of Reference created
 - Focused on building out strong IT audit capabilities and it is understood that the domains of privacy and security would be included
 - Primarily focused on internal (Ministry) compliance
- Financial compliance function is also under development and may be launched in parallel
 - Currently a formal linkage has not been established between these compliance roles, but synergies may exist
 - Synergies also likely exist in the reporting structure

Mandate – Initial areas of focus

- Based on recommendations from recent investigations and assessments, the following compliance areas should be considered (see following slides for additional detail):
 - 1) Internal Ministry compliance to relevant regulations, policies and directives
 - 2) Internal Ministry compliance to contractual obligations arising from inbound information sharing agreements
 - 3) Third-party compliance with Ministry terms outlined in outbound information sharing agreements
- Further, within each area, the domains of information security and privacy should be considered

1) Internal Ministry compliance with Policy and Legal requirements

- A risk-based approach to monitoring and assessing compliance with:
 - Relevant legislation
 - Examples include FOIPPA, Pharmaceutical Services Act, E-Health Act, etc.
 - Note that the applicability of legislative requirements is situation-specific
 - Relevant policies
 - Examples include the Information Security Policy, Core Policy & Procedures Manual, the Ministry Privacy Policy, etc.
- Key inputs to support an organization-wide assessment of risk and priority include:
 - Findings from recent incidents, investigations and assessments
 - Recent STRA and PIA results outlining remediation requirements and next steps

2) Internal Ministry compliance with inbound Information Sharing Agreements

- The Ministry establishes agreements with third parties in order to obtain access to relevant data to support analysis and decision-making activities
- Such agreements typically include terms for the protection of data which the Ministry is required to comply with
- In order to enable the Ministry to ensure it is complying with these requirements the mandate of the compliance function should include monitoring and reporting of performance against these terms (on a risk basis)
- Where third parties request the ability to audit Ministry compliance to these terms, the compliance function may support and/or coordinate these activities

3) Compliance of third parties to Ministry terms and conditions in outbound sharing agreements

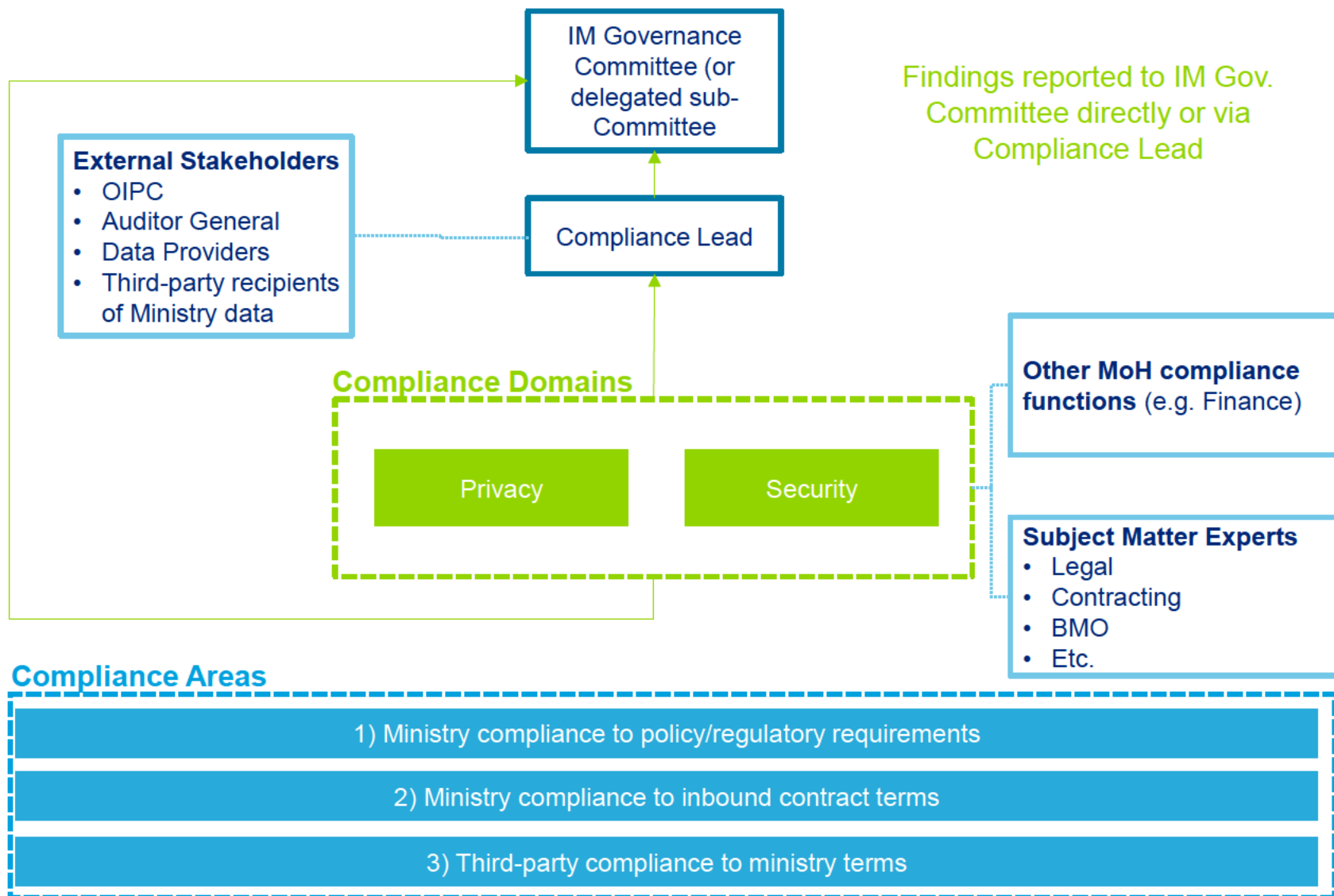
- Risk-based approach to assessing compliance of third parties to Ministry requirements defined in information sharing agreements
 - Criteria to consider for risk assessment include historical performance, the level of sensitivity of the data being provided, the volume of data being provided and the perceived quality of controls in place within the organization's environment (among others – the existing “risk ruler” could be used to support this process)
 - Requirements defined in the Ministry's information sharing agreements provide the criteria against which organizations can be audited by the compliance function to ensure compliance with Ministry requirements
- Third party self-assessments may be considered as an initial step in engaging this community and as a mechanism to support initial risk assessment and prioritization

Governance considerations

Compliance governance

- As noted above, compliance functions are often tasked with both an advisory and monitoring role
- While both roles can deliver significant value and support enhanced compliance, there is a need for the governance of the function to address the requirement for independence. Governance:
 - Defines accountabilities and reporting relationships associated with the compliance function
 - Is critical in order to clearly address the questions of “authority” and “independence”
- Ultimately, the compliance function must provide an enterprise-level, objective view of compliance status and risks through regular oversight, monitoring, reporting and follow up
- There are numerous options for addressing this challenge, and formally identifying and addressing specific risks to independence can support a pragmatic approach
 - As noted by HIPSL, the separation of the advisory role and the oversight/monitoring role within HIPSL may address this challenge if augmented by the proper reporting relationships to a Compliance Lead and Executive oversight body

Key compliance functions and reporting relationships



Implementation strategy considerations

Implementation strategy - considerations

- The implementation strategy defines the prioritized, time-based approach to implementing the function in alignment with the mandate
- While there are many parameters to consider when implementing a compliance function, five are useful for supporting clarity on objectives and setting and managing stakeholder expectations given limited resources:
 - Scope (Internal / External)
 - Perspective
 - Risk level
 - Coverage
 - Depth

Parameters

- **Scope:**

- Internal vs. External
 - As noted above, the compliance function will likely focus on the monitoring of compliance of both the Ministry (internal) and third parties (external)
- Selection of systems and data repositories to be covered
- Selection of functional areas and business processes to be covered

- **Perspective:**

- *Historical*: Review historical processes and documentation which may span multiple processes and/or responsible personnel; typical period of review is 6 months to a year.
- *Current state*: Review current processes and documentation; typical period of review is limited to 3 months or less (e.g. iSmart Health Check).
- *Future state*: Review the future design of processes; typically these are projects that will impact processes and procedures (e.g. remediation/enhancement projects, process re-design, system implementation requiring a PIA or STRA, etc.).

Compliance Strategy Levers – Areas of Focus (2 of 2)

- **Risk Level**

- Extreme, High, Moderate, Low risk
- Leverage existing risk assessments (e.g., risk ruler, investigation results, third-party recommendations) to support prioritization

- **Coverage:**

- Approach to determining how much assurance is needed to evaluate the ministry's overall level of compliance.

- **Depth:**

- *Design*: Review of the design and implementation of process and controls. A design review is intended only to evaluate if the process is designed to mitigate the risk of non-compliance.
- *Operating Effectiveness*: Review of the design, implementation and operating effectiveness of process and controls over a period of time. An operating effectiveness review is intended to determine whether there is evidence of non-compliance over a period of time.

Sample implementation strategy

- Based on the above, an implementation strategy can be developed to support the Ministry's objectives in each year
- Recognizing the immediate need to address high-risk compliance areas, a risk assessment would support the allocation of resources and effort to the organizations, systems and environments with the highest risk
- Once the assessment is complete and compared against available resources, any gaps can be identified, and the audit plan can be adjusted as required (with direction from, and approval of, an Executive oversight body)
- A sample strategy based on these five parameters is outlined below

	Fiscal 2014		Fiscal 2015		Fiscal 2016	
Scope	Internal	External	Internal	External	Internal	External
Perspective	Historical/ Current	Historical/ Current	Historical/ Current	Historical/ Current	Historical/ Current	Historical/ Current
Risk	Extreme and High	Extreme and High	Extreme, High, Moderate	Extreme, High, Moderate	Extreme, High, Moderate	Extreme, High, Moderate
Coverage	100%	100%	75% Extreme / High; 50% Moderate	75% Extreme / High; 50% Moderate	50% Extreme / High; 50% Moderate	50% Extreme / High; 50% Moderate
Depth	Design	Design	Operating Effectiveness	Operating Effectiveness	Operating Effectiveness	Operating Effectiveness

Implementation strategy considerations

- Risk assessment and prioritization
 - Key inputs for the baseline risk assessment include investigation findings, OIPC recommendations, Deloitte recommendations and PIA/STRA results
 - Consider focusing initially on providing an objective view of compliance, particularly against recommendations where the Ministry has made a public commitment to accept and address these recommendations
 - The compliance function can objectively monitor and report on progress and support follow up interactions with key external stakeholders
 - For External compliance - leverage existing risk ruler if possible and identify top risk areas
 - For low-risk agreements consider self assessment and sample-based audits. Align this with overall ISA refresh process

Implementation strategy considerations

- Prioritization and resourcing
 - With eight divisions and hundreds of ISAs, the compliance group will be overwhelmed very quickly
 - Initial prioritization will be critical to:
 - Obtaining agreement on areas of focus
 - Setting appropriate expectations
 - Identify lead compliance auditors and leverage SMEs and capacity elsewhere where possible
- Leverage the benefits of expected compliance monitoring
 - Announce the compliance function and its mandate
 - Initiate a self-reporting and sample-based compliance approach
 - Communicate assessment results

Implementation strategy considerations

- Deployment and communications
 - When communicating the launch of the function, consider including:
 - An overview of the mandate (and the availability of advisory support where requested)
 - A description of roles and responsibilities for:
 - The compliance function
 - Internal participants (prior to, during and after an assessment)
 - Executive oversight committee
 - External stakeholders
 - A description of the consequences of non-compliance

Implementation strategy considerations

- Key supporting tools and processes
 - Compliance policy and policy guidance
 - Education and awareness
 - Communication
 - Advisory support
 - Reporting (internal and external stakeholders)

Deloitte.