Internal Review

Ministry of Health, Pharmaceutical Services Division, Research and Evidence Development

September 26, 2013

Initial Draft - Confidential for Discussion October 1st

Insert letter from DM here

Contents

Executive Summary

The Office of the Auditor General (OAG) received allegations late March 2012 regarding: (1) inappropriate data access arrangements and intellectual property infringements, (2) irregular procurement, contracting and research grant practices, and (3) Standards of Conduct Policy conflicts and preferential treatment in employee-contractor relations in the Pharmaceutical Services Division (PSD).

An internal investigation was launched into these allegations. A team of representatives from the government Chief Information Office, the Public Service Agency (PSA), and the Ministry of Health's Financial Services Division and Health Sector Information Management and Technology Division were tasked with conducting this investigation. The investigative activities included, but were not limited to:

- Review of electronic communications of relevant parties,
- Review of related project documents,
- Interviews with relevant parties,
- Assessment of identified individuals' data access, use and disclosure and related agreements,
- Review of identified individuals' data sharing and disclosure activities,
- Review of procurement practices, grant awards and contracting,
- Assessment of intellectual property rights for employees and contractors identified through the course of this investigation.

s.22

In the fall of 2012, the Office of the Comptroller General (OCG) and the Royal Canadian Mounted Police (RCMP) were contacted and informed of the initial findings of the review. The OCG has since launched a parallel investigation, the outcome of which is still pending. The RCMP is awaiting the outcomes of this and the OCG's investigation to commence any formal investigation.

The key findings of this investigation led to a number of lessons learned on what needs to be accomplished to improve the policies and processes for employee, researcher and contractor data access to improve data security and privacy protections, as well as, recommendations to further develop protocols for the contracts and grants awarded by the Ministry. The recommendations found herein strive to supplement the recommendations to improve the Ministry's data security and privacy protections already provided in the reports issued in June 2013 by Office of the Information and Privacy Commissioner for British Columbia and the consulting firm Deloitte.

Introduction

Background

The Office of the Auditor General (OAG) contacted the Assistant Deputy Minister (ADM) of Financial and Corporate Services, Ministry of Health (hereafter referred to as "the Ministry") on March 28, 2012 to advise that an allegation had been received by their office concerning inappropriate procurement, contracting irregularities and research grant practices in the Research and Evidence Development section of the Ministry's Pharmaceutical Services Division (PSD).

Additional concerns were also alleged regarding inappropriate data access arrangements, intellectual property infringement, and code of conduct conflicts with employee contractor relationships including preferential treatment. At that time Ministry undertook a preliminary review. As a result of the preliminary review, Ministry determined that further investigation was warranted and decided to undertake a more detailed review of the allegations.

Project Team

A team of representatives from the government Chief Information Office, the Public Service Agency (PSA), and the Ministry of Health's Financial Services Division and Health Sector Information Management and Technology Division were tasked with conducting this investigation.

Key Work Elements

The purpose of this review was:

- To provide findings related to allegations;
- To determine if Government's contracting and research grant practices, standards of conduct, data access arrangements and approval processes are being followed by the identified staff and contractors; and
- To identify opportunities and make recommendations to improve contracting, granting, and data access practices across the Ministry.

The investigation was had two phases – Phase I focused on the activities of ministry employees and the efforts to support the resulting litigation and arbitration; Phase II focused on the activities of contractors utilizing ministry data. The investigative activities included, but were not limited to:

- Review of electronic communications of relevant parties,
- Review of related project documents,
- Interviews with relevant parties,
- Assessment of identified individuals' data access, use and disclosure and related agreements,
- Review of identified individuals' data sharing and disclosure activities,
- Review of procurement practices, grant awards and contracting,

- Assessment of intellectual property rights for employees and contractors identified through the course of this investigation.

The legislative and policy context, a chronology of events, key findings of the investigation and recommendations to enhance data security and privacy protections and mitigate the reoccurrence of such incidents are covered in this report.

Legislative and Policy Context

The investigation was conducted within a legislative framework that includes:

- The *Financial Administration Act,*
- The *Procurement Services Act,*
- The *Freedom of Information and Protection of Privacy Act,*
- The *Pharmaceutical Services Act* ,
- The *Pharmacy Operations and Drug Scheduling Act,*
- The *E-Health (Personal Health Information Access and Protection of Privacy) Act* ,
- The *Vital Statistics Act, and*
- The *Public Service Act.*

The applicable policies cited for this investigation include, but are not limited to:

- The B.C. Government Standards of Conduct,
- The Core Policy and Procedure Manual, and
- The Information Security Policy.

As the Canadian Community Health Survey data was involved in the investigation, we also had to review findings within the framework of the *Agreement Concerning the Collection and Sharing of Information from the Canadian Community Health Survey between Statistics Canada and the British Columbia Ministry of Health.*

For specific details on the legislation and policy provisions that provide the framework for this review, please refer to **Appendix 1 – Legislation and Policy**.

Chronology of Events

At the end of March 2012, the Office of the Auditor General informs the Ministry that someone made allegations about the: (1) inappropriate data access arrangements and intellectual property infringements, (2) irregular procurement, contracting and research grant practices, and (3) Standards of Conduct Policy conflicts and preferential treatment in employee-contractor relations in the Pharmaceutical Services Division (PSD). The Ministry commenced a preliminary review of the matters alleged in April 2012 and determines that further action is warranted. Subsequently, the formal internal investigation into these allegations began in May 2012.

In July 2012 the investigation team produced an interim update of the key findings to the Deputy Minister of Health. Furthermore, data access was suspended for identified employees and contractors and associated contracts were also suspended. As the investigation progressed through the following months and more key evidence was obtained, identified employees were dismissed and contracts terminated.

In September 2012 the Ministry issues a press release making a public announcement of this investigation.

In October the Ministry sends letters to identified employees and contractors requiring the return of Ministry data and information and requests to sign declarations that letter recipients do not possess or have in their custody or control Ministry data and/or information. The Ministry received responses to these letters throughout the fall of 2012.

In January 2013 the Ministry notified 35,480 affected individuals of a privacy breach involving their personal information and also published a general public notification of two other privacy breaches. A contact centre was developed to provide telephone response to inquiries from affected B.C. residents.

In March 2013 the investigation team switched their focus from employees to appropriate access and use of data by identified third party contractors, researchers and university-based projects. Additional letters were sent to these contractors/researchers and responses were received by the Ministry through the summer of 2013.

For a detailed timeline of the investigation, please refer to **Appendix 2 – Investigation Timeline.**

Summary of Key Findings and Facts

The following is a summary of findings based on the review of electronic communications, project documents, interviews data access, use and disclosure and related agreements, data sharing and disclosure activities, procurement practices, grant awards and contracting, intellectual property rights for employees and contractors identified through the course of this investigation.

Contract Management and Grants

The following issues have been identified regarding the arranging, awarding and subcontracting of contracts in the PSD Research and Evidence Development:

s.22

s.22

- There was a disparity between the development of research contracts with university-based researchers and the development of resulting data access and information sharing agreements.
- There was limited capacity and information on references and background details on contractors from universities and other public bodies. Confidentiality pledges and other personal statements collected by universities were not always provided, reviewed nor approved by the Ministry.

Data Access and Use

The following findings were identified relating to the use and access to data:

- Processes for data access were not always followed and there is a lack of documentation for projects. s.22

- Employees were using their Ministry data access privileges to support colleagues in their research/contracting endeavors without proper authorization to use the data for these purposes resulting in major privacy breaches requiring the notification of British Columbians and an independent investigation by the OIPC. In these incidents personal health data was inappropriately accessed, saved on portable storage devices (USB sticks) and shared with researchers and/or contractors without required permissions and protocols being followed.
- Some contracts were overly general in the scope of evaluation and project work required. Consequently ISAs were developed that generally enabled contractors' open use of data for other projects and evaluation work.
-

s.22

- There was insufficient capacity for and completion of cataloguing, auditing, monitoring and enforcement of ISAs, similar data access agreements, and employee data access privileges within Ministry.
-

s.22

s.22

- Researchers and contractors are not sufficiently aware of or were aware but not using the existing open data resources publicly available from the Ministry.

Standards of Conduct

The following issues relating to breaches of the Standards of Conduct for the BC Public Service

s.22

Subsequent Actions Taken

The key findings of the investigation led investigators to the conclusion on legislative, policy and agreement violations described above. Consequently, the ministry took actions with respect to specific employees and contracts.

Over the past year, the Ministry has improved its data security and access processes and procedures. Ministry also accepted and began implementing recommendations from the Office

of the Information and Privacy Commissioner's (OIPC) report on their independent investigation, and from the information security review by consulting firm Deloitte.

A copy of Delloite's report is available on the Ministry website at: http://www.health.gov.bc.ca/cpa/mediasite/pdf/deloitte-report.pdf

A copy of the OIPC's report is available on their website at: http://www.oipc.bc.ca/news-events.aspx?Status=Archived

Work that is already underway or completed by Ministry includes:

- More than 280 managers and executives at the Ministry have completed mandatory privacy and data security training;
- All of the Ministry's divisions have reviewed and inventoried the sensitive data they have and how it is secured and protected; and
- The Ministry has improved its data warehousing system by decommissioning certain legacy system and restricting use of others. The data warehouse system now also has greater capacity log and actively monitor who is accessing which data.

Ministry is also actively working on or completing the following recommendations made by Deloitte and the OIPC:

- Other ministry, non-management, employees will undergo the enhanced privacy and data security training, in addition to training already required for all public servants;
- Ministry user privileges are granted and managed based on the need to know and least privilege principles, ensuring that employees have access only to the minimum amount of personal information they require to perform their employment duties. Access permissions are being assigned consistently and kept up to date;
- Access to older, outmoded software used to work with data has been severely restricted - this software is in the process of being replaced with more modern, more secure programs; and
- The Ministry is developing easy-to-understand reference guides and other materials for staff on data security and privacy.

Recommendations

A number of lessons have been learned throughout the course of this investigation on what needs to be accomplished and implemented to improve the policies and processes for how the Ministry grants contracts, and how employees, researchers and contractors access data.

Further to the findings and recommendations in the OIPC and Deloitte's respective reports, the findings of this investigation have provided important lessons learned. The following are recommendations for the Ministry in working with researchers, universities, and contractors, as to maintain public trust through fairness in government procurement practices and further enhancement of data security and privacy protections.

Ministry:

1. Ministry should develop a broader open health data strategy to make more useable aggregate health data readily available to contractors, researchers and the public.
2. Ministry should develop and implement a secure data access and use environment for researchers, contractors and employees to enhance capacity for research, policy development and potential revenue generation.
3. Health Sector IM/IT Division should conduct ongoing audit and monitoring for legacy systems, and decommission these legacy systems as soon as possible.
4. Ministry should develop and disseminate standard definitions and classification structures for different levels of data (open data, aggregate data, de-identified row level data, identifiable row level data, identified row level data and any other applicable levels of data).
5. Health Sector IM/IT Division should periodically review all Ministry LAN drives to ensure that employees and contractors only have access to information they require for their roles and responsibilities and to ensure that personal health information is stored appropriately and not accessible to unauthorized individuals.
6. Health Sector IM/IT Division should develop a more robust process for auditing data access for ministry staff and contractors so that when internal data access requests are being reviewed and approved by managers in a way that limits data access based on the principles of least privilege and need to know for the employee/contractors' role(s). This process must address the need to adapt data access permission when staff and contractors move within the ministry to different roles requiring different data access permissions.
7. Ministry should develop clearly stated and strictly enforced consequences for employees, researchers, contractors and anyone else not complying with the requirements of legislation, corporate data policies and procedures or legal provisions in contracts and ISAs.
8. s.22
9. Contracts requiring access to and use of data should be developed in unison with ISAs by an integrated, collaborative effort of all the required subject matter experts.
10. That the IDIR accounts for external contractors when required be identified as contractors in the Public Service Directory and an external email identifier for IDIRs be issued – i.e. jane.smith@contractor.gov.bc.ca
11. Contracts requiring data should be developed in unison with the ISA and must have data access approval(s) in place prior to signing of contracts. ISAs should be included in the contract schedules.
12. All Ministry contractors are required to complete the new Privacy and Information Management training on line and provide copy of completion certificate before contracts and/or data is provided.
13. Ministry employees who are also employed by universities must not serve in dual roles wherein they conduct research or provide contracted services for MINISTRY.
14. Data access arrangements should only be granted for project specific or identified evaluation contracts, and data access is limited to information required and not for other, unauthorized uses.
15. All Data Access and Information Sharing Agreements (ISAs) should be located and tracked by Health Sector IM/IT division and ADM/Ministry CIO approval is required for all such agreements between the Ministry and external parties. This includes ongoing compliance audits of data storage, data return and/or data destruction provisions listed in agreements.

16. Ministry should develop a robust compliance and monitoring function for data access, logging, tracking and auditing. Ideally with an independent and integrated unit dedicated to the continuous monitoring, auditing and compliance regarding the access, storage, use and disclosure of Ministry data with internal staff, other government employees, researches, contractors and external agencies.
17. Health Sector IM/IT Division should provide clear guidance on proper data access processes and sufficient resources for a client-centric, streamlined data access model so that data clients do not feel the need to circumvent current data access procedures.
18. Health Sector IM/IT Division should conduct periodic reviews of data access processes and procedures and provide training to all divisions after completion to ensure all proper processes are in place in all business areas with a focus on personal health information, eHealth, pharmaceutical data, health data legislation and any other personal information protection requirements.
19. Ministry employees should be required to review and sign-off on the BC Public Service Standards of Conduct IM/IT agreement annually to ensure they are aware of their responsibilities as employees and the policies and procedures for data access, including a reminder that they must not share IDIR passwords or data access information with others. Other ministries do this with annual Employee Performance Development Plan (EPDP) discussions.
20. All new Ministry employees should be required to take government privacy and information sharing training and Ministry information privacy and security training prior to having data access.
21. All Ministry employees handling sensitive health information should be issued an encrypted USB stick for any work requiring external information storage and be trained on appropriate data storage methods.
22. Ministry should conduct regular audits of password usage for individuals who have access to personal health information data bases to ensure no one else is using their credentials.
23. Ministry should develop greater awareness of the pre-publication review process required for researchers and contractors with permission to publish.

Universities:

24. Ministry should work with universities to ensure that contracted staff is aware of and adhere to the data security and privacy protection provisions in contracts and relevant agreements.
25. University-based researchers providing services to the Ministry must also complete the contractor privacy and information managements training.
26. Contracts with universities for service(s) involving research or analysis of Ministry data should require a listing of all researchers/contractors on the project for review by the Ministry before data is issued. Universities are responsible for ensuring that any and all university staff involved in providing contracted services to the MINISTRY are listed on agreements or contracts, including ISAs, are free from conflict of interest, such as those serving in dual roles for the university conducting research on MINISTRY projects, and any pledge forms are provided to the Ministry for review and approval prior to granting data access.

27. Data access arrangements will only be granted for project specific or identified evaluation contracts, and data access is limited to information required and not for other, unauthorized uses.
28. Ministry should develop over-arching research agreements with major universities involved in health research to formalize and create greater awareness of the expectations, roles, and responsibilities around the appropriate access, use, storage and disclosure of health data.

Contractors:

29. Prior to singing a contract, all contractors must provide a Conflict of Interest statement and consent for reference checks.
30. All contractors should clearly identify their relationship to the Ministry when dealing with any third party organization.
31. All Ministry contractors are required to complete the new Privacy and Information Management training on line and provide copy of completion certificate before contracts and/or data is provided.
32. Data access arrangements should only be granted for project specific or identified evaluation contracts, and data access is limited to the project or evaluation and not for other, unauthorized uses.
33. Ministry should collaborate with other stakeholders across government to improve the capacity to review and assess potential contractors' previous work history, performance metrics and references with other ministries and public bodies, upon receiving consent to check references from contractors.
34. Contractors should be made aware that they are not permitted to forward email to personal non-government email and/or store Ministry data on personal computers.
35. All contractors handling sensitive health information should be required to only use encrypted portable storage devices when no viable alternative exists to the data being saved on the portable storage devices.
36. Contractors being granted data access must return and/or destroy the data they were provided within the data retention schedule specified in the contract.
37. Contractors should not be permitted to publish findings based on contracted work completed on or behalf of the Ministry.
38. All contracts should follow Ministry policies and process for Request for Proposals (RFPs) to solicit proposals for all projects. Requests for proposal should be written to allow for a fair and open competition without limiting the option to a single preferred service provider. RFPs should be on ability to provide service and on not experience with specific Ministry tools, resources, programs or data holdings.

Researchers:

39. All researchers should request their data through Population Data B.C.'s data access request (DAR) process.
40. All researchers wishing to publish and/or distribute their findings are required to include a proper citation of the source of their data and submit their manuscript or materials intended for distribution for pre-publication/distribution review and approval by the Ministry at least 45 days in advance publication.

41. Ministry should develop clear policies for non-compliance with the research agreements and other applicable legislation and corporate policies and make researchers aware of such policies and the consequences of non-compliance.
42. Research Agreements should explicitly state the roles and responsibilities for parties to the agreement, particularly the Principal Investigator, who must ensure:
    a. That all associated researchers to the project are aware of the expectations of care of Ministry data and after accessing, using, storing and, where appropriate, disclosing Ministry in a manner consistent with legislation, policy and the provisions of the research agreement,
    b. All researchers associated with research projects are clearly identified and have submitted their conflict of interest and confidentiality statements,
    c. All required data elements need to be specifically outlined in the DAR, and based on the principles of 'least privilege' and 'need to know',
    d. All developed publications or materials for distribution undergo the Ministry's pre-publication review process, and
    e. All researchers associated with the project participate in Ministry's online privacy and information management training as required.

Appendix 1 – Legislation and Policy Violations

The key findings of this investigation led investigators to numerous conclusions and subsequently actions related to former employees and contractors for violations of the following legislative, policy and agreement provisions:

Public Service Act

8 Appointments on Merit

(1) Subject to section 10, appointments to and from within the public service must
(a) be based on the principle of merit, and
(b) be the result of a process designed to appraise the knowledge, skills and abilities of eligible applicants.

(2) The matters to be considered in determining merit must, having regard to the nature of the duties to be performed, include the applicant's education, skills, knowledge, experience, past work performance and years of continuous service in the public service.

10 Exceptions to section 8

Subject to the regulations
(a) section 8 (1) does not apply to an appointment that is a lateral transfer or a demotion, and
(b) section 8 (1) (b) does not apply to the following:
(i) a temporary appointment of not more than 7 months in duration;
(ii) an appointment of an auxiliary employee;
(iii) a direct appointment by the agency head in unusual or exceptional circumstances.

Freedom of Information and Protection of Privacy Act

30 Protection of personal information

A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

32 Use of personal information

A public body may use personal information in its custody or under its control only
(a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34 for "consistent purpose"),
(b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or
(c) for a purpose for which that information may be disclosed to that public body under sections 33 to 36.

35 Disclosure for research or statistical purposes

(1) A public body may disclose personal information in its custody or under its control for a research purpose, including statistical research, only if

...

(c) the head of the public body concerned has approved conditions relating to the following:

(i) security and confidentiality;

(ii) the removal or destruction of individual identifiers at the earliest reasonable time;

(iii) the prohibition of any subsequent use or disclosure of that information in individually identifiable form without the express authorization of that public body, and

(d) the person to whom that information is disclosed has signed an agreement to comply with the approved conditions, this Act and any of the public body's policies and procedures relating to the confidentiality of personal information.

Pharmacy Operations and Drug Scheduling Act

13 Continuation of PharmaNet

(1) The minister may continue the Provincial computerized networks and associated databases, collectively known as PharmaNet, for the purpose of facilitating(i) scientific, health service delivery or drug use research conducted at a university or hospital, or as approved by the PharmaNet stewardship committee, and

(j) health policy research, planning or evaluation related to drug use, pharmacare or health service delivery.

16 Disclosure of PharmaNet patient record information

(2) Subject to the rules, the PharmaNet stewardship committee may disclose to a person, for the purposes described in section 13 (1) (i) or (j), information recorded in a PharmaNet database that would be personal health information, except that the information disclosed must not include patient or practitioner names, addresses or other information that could allow a patient or practitioner to be identified or contacted.

Standards of Conduct

Confidentiality:

Confidential information, in any form, that employees receive through their employment must not be disclosed, released, or transmitted to anyone other than persons who are authorized to receive the information.

Confidential information that employees receive through their employment must not be used by an employee for the purpose of furthering any private interest, or as a means of making personal gains.

Conflict of Interest:

Examples of conflicts of interest include, but are not limited to, the following:

...

- *An employee, in the performance of official duties, gives preferential treatment to an individual, corporation, or organization, including a non-profit organization, in which the employee, or a relative or friend of the employee, has an interest, financial or otherwise;*
- *An employee benefits from, or is reasonably perceived by the public to have benefited from, the use of information acquired solely by reason of the employee's employment; and/or*
- *An employee benefits from, or is reasonably perceived by the public to have benefited from, a government transaction over which the employee can influence decisions (for example, investments, sales, purchases, borrowing, grants, contracts, regulatory or discretionary approvals, appointments);*

Outside Remunerative and Volunteer Work:

Employees may hold jobs outside government, carry on a business, receive remuneration from public funds for activities outside their position, or engage in volunteer activities provided it does not:

...

- *Gain an advantage that is derived from their employment with the BC Public Service.*

Allegations of Wrong Doing:

Employees have a duty to report any situation relevant to the BC Public Service that they believe contravenes the law, misuses public funds or assets, or represents a danger to public health and safety or a significant danger to the environment... Employees must report their allegations or concerns as follows:

- *Members of the BCGEU must report in accordance with Article 32.13;*
- *PEA members must report in accordance with Article 36.12; or*
- *Other employees must report in writing to their Deputy Minister or other executive member of the ministry, who will acknowledge receipt of the submission and have the matter reviewed and responded to in writing within 30 days of receiving the employee's submission. Where an allegation involves a Deputy Minister, the employee must forward the allegation to the Deputy Minister to the Premier.*

Loyalty:

Public service employees have a duty of loyalty to the government as their employer. They must act honestly and in good faith and place the interests of the employer ahead of their own private interests. The duty committed to in the Oath of Employment requires BC Public Service employees to serve the government of the day to the best of their ability.

Core Policy and Procedure Manual:
Chapter 12 - Information Management and Information Technology Management Policy

12.3.1 a) Appropriate Use of Information Technology

...
Users must not:
...

- *divulge, share or compromise their own or another's government authentication credentials;*

12.3.3 d) Personal Information Management

4. Ministries must use the principles of "need-to-know" and "least privilege" when authorizing access to personal information.

- *Least privilege* is defined as: *"A security principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error or unauthorized use".*
- *Need to know* is defined as: *"A privacy principle where access is restricted to authorized individuals whose duties require such access. Individuals are not entitled to access merely because of status, rank or office".*
- *The need-to-know principle may be implemented in various ways. These include physically segregating and controlling access to certain records, listing individuals who may access certain records, or installing access controls on automated information systems.*
- *The need-to-know principle is especially important in protecting the privacy of individuals as required by the Freedom of Information and Protection of Privacy Act."*

12.3.6. a) Information and Technology Security

4. Users of government assets must continue to be aware of, and understand, their role in reducing the risk of theft, fraud or misuse of government assets...

9. Data and information exchanges within government, or with an external entity, must be secure and managed through a documented process

Information Security Policy

6.7.1 b) Use of portable storage devices

The use of portable storage devices to store or transport information increases the risk of information compromise. Portable storage devices are typically small, portable and are easily lost, stolen or damaged, particularly when transported in public environments.

Information Owners, Information Custodians and Managers must:

- *Ensure that use of portable storage devices is managed and controlled to mitigate risks;*
- *Document processes for authorizing use of portable storage devices; and,*
- *Ensure personnel using portable storage devices protect information and information technology assets in their custody or control.*

6.10.1 a) Audit logging

Information Owners and Information Custodians must ensure that audit logs are used to record user and system activities, exceptions and information security and operational events including information about activity on networks, applications and systems. Information Owners and Information Custodians will determine the degree of detail to be logged based on the value and sensitivity of information assets, the criticality of the system and the resources required to review and analyze the audit logs. Audit logs should include, where relevant, the following information:

- *User identifier;*
- *Dates, times and details of key events (e.g., logon and logoff);*
- *Logon method, location, terminal identity (if possible), network address;*
- *Records of successful and unsuccessful system access attempts;*
- *Records of successful and unsuccessful data access (including record and field access where applicable) and other resource access attempts;*
- *Changes to system configuration;*
- *Use of privileges;*
- *Use of system utilities and applications;*
- *Files accessed and type of access (e.g., view, read, modify, delete);*
- *Network addresses and protocols;*
- *Alarms raised by the access control systems (e.g., anti-virus, intrusion detection).*

Audit logs may contain confidential data and access must be restricted to personnel with 'need-to-know' privileged access and be protected accordingly.

Information Owners and Information Custodians must not have the ability to modify, erase or de-activate logs of their own activities.

If audit logs are not activated, this decision must be documented and include the name and position of the approver, date and a rationale for de-activating the log. Where required, the Privacy Impact Assessment and/or Security Threat and Risk Assessment must be updated to reflect this decision.

7.3.1 d) Protection and use of passwords

Passwords are highly sensitive and must be protected by not:

- *Sharing or disclosing passwords;*
- *Permitting anyone to view the password as it is being entered;*
- *Writing down a password;*

- *Storing other personal identifiers, access codes, tokens or passwords in the same container as the token;*
- *Keeping a file of passwords on any computer system, including mobile devices unless that file is encrypted according to the Cryptographic Standards for Information Protection; and*
- *Employing any automatic or scripted logon processes for personal identifiers; and,*
- *Using personal identifiers, access codes, or passwords associated with Government accounts for non-government purposes.*

7.7.1 a) Information protection paramount

Information Owners and Information Custodians must ensure that use of portable storage devices is managed and controlled to mitigate the inherent risks of portable storage devices.

The use of portable storage devices such as laptops or other mobile devices to access, store, or process information increases the risk of information compromise. Portable storage devices are typically small, portable, used in uncontrolled public environments and are easily lost, stolen or damaged.

...

Users of mobile computing services must ensure that information and information technology assets in their custody or control are protected.

7.7.1 c) Protection of credentials

User identifiers and user credentials must be protected to reduce the risk of unauthorized access to information and information technology assets.
In particular, users must protect against visual eavesdropping of passwords, PINs and other credentials, especially when in public places.

7.7.1 f) Risk assessment factors

Information classification and sensitivity levels must be considered in the risk assessment.

Minimum information protection safeguards for the use of portable storage devices include:

- *Encryption of stored data to prevent information loss resulting from the theft of the mobile or remote device;*
- *Encryption of data transmitted via public network;*
- *Access control permissions on a portable storage device must be applied to prevent unauthorised access to information by system users, particularly for multi-user mobile systems;*
- *Regularly maintained data backups of information stored on portable storage devices using government backup facilities to protect against information loss;*

- *To provide information availability portable storage devices must not be used to store the only copy of a government record;*
- *Physical security of the device must be maintained to protect against asset and information loss; and,*
- *User authentication to the portable storage device and user authentication for remote access from the device must be implemented in accordance with authentication policies.*

Agreement Concerning the Collection and Sharing of Information from the Canadian Community Health Survey Between Statistics Canada and the British Columbia Ministry of Health

4 Usage of Shared Information

(3) The Ministry shall consult with Statistics Canada prior to releasing any statistical aggregates to prevent any residual disclosure of information.

5 Confidentiality of Data

The information shared with the Ministry pursuant to this Agreement relating to an identifiable respondent shall be treated as confidential and the Ministry shall take such steps as are necessary to protect this information.

6 Sharing with Third Party

The Ministry shall not, by agreement or otherwise, share with or disclose to any other party the individual responses obtained from respondents and shared pursuant to this Agreement except in accordance with the following:

...

(2) The Ministry may provide access to the individual survey responses, without any names, addresses or identifying numbers, shared pursuant to this Agreement to a researcher, working under contract directly for the Ministry to provide a survey-related product or service, provided such access is on the premises of the Ministry where the required security measures are in place to protect the confidentiality of the information relating to the individual identifiable respondents.

Appendix 2 – Investigation Timeline

March 28, 2012	The Office of the Auditor General contacts the Ministry to advise that someone has made an allegation about contracting irregularities and inappropriate research practices in the PSD.
April 2012	Ministry undertakes a preliminary review of the matters alleged to determine if further action warranted.
May, 2012	Based on results of preliminary review, Ministry initiates an official internal investigation.
July 18, 2012	Ministry internal investigation team produces an interim update for the Deputy Minister.
July / August 2012	Ministry representatives have initial meeting and discussions with UVIC and UBC representatives regarding the investigation and affected university contracts and research programs.
September 6, 2102	Ministry issues press release and Minister of Health and Deputy Minister of Health make public announcement about the internal investigation.
September 19, 2102	Ministry sends letter to UVIC and UBC notifying them of the suspensions of certain Ministry sponsored projects/research studies.
October 31, 2012	Ministry sends demand letters requiring return of Ministry data and information and requesting signing of a declaration that individual does not have possession, custody or control of Ministry data and information.
November 5, 2012	Ministry sends more demand letters and declarations.
November 2012	Ministry receives signed declaration letters.
December 11, 2012	Ministry resumes funding for a temporarily suspended research study.
January 16-22, 2013	Ministry notifies 35,480 affected individuals of a privacy breach involving their personal information. Ministry provides general public notification of two other privacy breaches. Ministry establishes a contact centre providing telephone response to inquiries.

Beginning March 2013	Ministry investigation continues reviewing third party contractors and researchers and review of University projects and data access.
August 1-2, 2013	Demand letters are sent to other identified Ministry of Health contractors
September 2013	Ministry receives responses to demand letters from contractors.
End of September 2013	This report is drafted.

Pages 24 through 35 redacted for the following reasons:
- -
s.14
s.14, s.17
s.14, s.22