CFR-2021-12563:

A list of all privacy impact assessments completed regarding the province's electronic health records (EHR) system, with a brief description of each and the date that they were completed.

iEHR Release 3 implementation PIA – March 3rd 2010

This PIA is an addendum to the *iEHR-PLIS Release 2 Design PIA (October 2009)*. It continues point-intime assessments of BC's interoperable Electronic Health Record ("iEHR") solution coinciding with material changes to ensure privacy risks are not introduced or previously known risks made worse. Whereas previous PIAs examined the design of the iEHR privacy functionality and controls, such as disclosure directives and the eHealth Access Model, this PIA is focused on the physical environment and the privacy management and controls in the production environment being introduced with Release 3 of the iEHR solution.

iEHR-PLIS release 2 design PIA – January 25th, 2010

Authorization page for the iEHR-PLIS Release 2

BC_iEHR PLIS design PIA Nov 11, 2008

The purpose of this Integrated Design Interoperable Electronic Health Record-Provincial Laboratory Information Solution (iEHR-PLIS), Privacy Impact Assessment (PIA) is to discuss the design-level privacy and security functionality that will comprise Release 1.1a of the BC iEHR-PLIS solution, which is part of Phase 2.1 of the BC iEHR-PLIS Project. The PIA identifies privacy and security risks and makes recommendations to mitigate those risks.

Community Lab Onboarding PIA – August 13, 2012

"Onboarding" refers to bringing a new source of diagnostic information into the Province's interoperable Electronic Health Record ('iEHR'). The Community Lab Onboarding to iEHR-PLIS Project ('Project') will implement and operationalize support for a near real-time feed of BC Biomedical Laboratories, LifeLabs Medical Laboratory Services, and Valley Medical Laboratories (collectively 'Community Labs') test result data to the iEHR Provincial Laboratory Information Solution ('PLIS') data repository; from which it can be accessed by authorized iEHR users.

2015-20 PLIA QA consultant – May 8th 2015

This initiative update to the E-Health PIA for Medical Practice Access to PLIS and HIAL: EMR-HER Integration Project describes consultant quality assurance activities to ensure PLIS data integrity.

2020-80 Hospital at Home – January 27, 2021

The purpose of this PIA is to provide a high-level overview and assessment of the HaH program which includes the provincial direction of the program including general collection, use and disclosure of personal information required for the delivery, management, operation, and evaluation of the program.

2020-57 MHSU Virtual Clinic App – Nov 6th, 2020

This PIA covers the Ministry of Health's technical support for the Shiftwell application through CGI and Freshworks. The development of the app itself is not being assessed in this PIA, which is addressed by PHSA's PIA

2020-32 Virtual Physician Pathways – January 13, 2021

This PIA covers the collection of personal information by the HEiDi vGP from the patient and the ecounter recorded for thos patients by the HLBC Registered Nursing team, that are entered into the MOIS shared EMR by the vMOA.

2018-36 MHSU Virtual Clinic – Dec 14, 2018

The scope of this PIA is to outline the Ministry of Health and Ministry of Mental Health and Addictions involvement in the MHSU Virtual Clinic project and the relationship between all participating parties.

BRITISH COLUMBIA

Privacy Impact Assessment for

MHSU Virtual Clinic

PIA#: HLTH18048 / **MoH#:** *2018-36*

Why do I need to do a PIA?
Section 69 (5) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a ministry to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA. Section 69 (5.1) requires the head to submit the PIA to the minister responsible for FOIPPA for review, during the development of any new system, project, program or activity, or proposed enactment, or when making changes to an existing one. The Privacy, Compliance and Training Branch (PCT) is the representative of the Minister for these purposes. Ministries must submit PIAs to PCT at pia.intake@gov.bc.ca for review and comment prior to implementation of any initiative. If you have any questions, please call the Privacy and Access Helpline (250 356-1851) for a privacy advisor. Please see our PIA Guidelines for question-specific guidance on completing a PIA.

What if my initiative does not include personal information?
Ministries still need to complete Part 1 of the PIA and submit it, along with the signatures pages, to PCT even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

Part 1 – General

Name of Ministry:	Ministry of Health		
PIA Drafter:	Shawna Lynch, Senior Privacy Analyst		
Email:	Shawna.Lynch@gov.bc.ca	Phone:	**778-974-2702**
Program Manager:	Jane London, Project Director		
Email:	Jane.London@gov.bc.ca	Phone:	**250-508-8374**

1. Description of the Initiative

The Mental Health and Substance Use (MHSU) Virtual Clinic project will create and pilot an innovative virtual clinic platform for online access to clinically supported evidenced-based online therapy and other support tools for individuals suffering from mild to moderate mental health and substance use problems.

The purpose of the Project is to complete a limited production rollout (LPR) of an innovative virtual clinic platform for delivering online counselling (virtual care) and other support tools to individuals suffering from mild to moderate mental health and substance use problems. A number of candidate organizations were approached by the Province and two (LPR Programs) have agreed to take part in project implementations using the platform:

- *Foundry, which provides integrated health and social services for young people; and*
- *The BC Emergency Health Services Commission (EHS) Critical Incident Stress Program which supports occupationally injured paramedics, dispatchers and families.*

Stakeholders from across government have worked to bring this initiative forward. Additionally, in 2016 the cross government Mental Health Secretariat (the Secretariat) worked on a provincial mental health approach to address gaps in the system of care, including an absence of tools to help individuals, patients and service providers navigate to credible MHSU information and access appropriate services.

The Secretariat recommended that the Ministry of Health (MoH) develop a proposal for an innovative project addressing these challenges and seize the opportunity offered by the Strategic Investment Fund (SIF). The SIF holds a portion of TELUS profits from providing telecommunications services to the Province and public sector partners and allows them to purchase TELUS services to support transformative technology projects with direct benefit to citizens. The MMHA and MoH will leverage the TELUS business relationship and corresponding SIF to provide the services in the MHSU initiative.

Strategic Investment Fund (SIF)

In June 29, 2011, a Notice of Intent (NOI) was posted to BC Bid outlining the Province's intention to award directly to TELUS for telecommunications and other services for a 10 year term, ending in 2021.

Within the framework of the Telecommunications Services Master Agreement (TSMA) and more specifically the Strategic Relationship Agreement (SRA) between TELUS and the broader public sector in BC, a portion of the revenues realized by TELUS for services provided are set aside in the Strategic Investment Fund (SIF). Eligibility to access these funds must be considered jointly by the Government, the broader public sector and TELUS and must be focused on leveraging technology and telecommunications services to enable ambitious, transformative initiatives designed to significantly benefit British Columbians. The use of the SIF provides an alternative path to typical government procurements. As the provider of the SIF, TELUS holds an integral role in the governance of the investments and the delivery of the funded initiatives. It is assumed that TELUS will be the primary provider of the proposed solution, as outlined in the SRA. The SIF is designed to enable innovation for the Province and also TELUS, developing and proving out what has never-been-done-before.

The Ministry applied for and received $5 million through the SIF for this proof-of concept project early 2018.

Partnerships

A number of candidate organizations were approached by the Province and two programs have agreed to take part in project implementations:

- *Foundry, which provides integrated health and social services for young people; and*
- *The BC Emergency Health Services Commission (EHS) Critical Incident Stress Program.*

The Ministry of Health and Ministry of Mental Health and Addictions are sponsoring this initiative in partnership with Foundry, BC Children's Hospital, Providence Healthcare, Provincial Health Services Authority, and BC Emergency Health Services. The Province and TELUS through SIF provide project management resources and the SIF covers the costs of the MHSU Virtual Clinic Limited Production Rollout.

Foundry: *Originally known as the BC Integrated Youth Services Initiative, was created in 2015. Foundry offers young people ages 12-24 health and wellness resources, services and supports, online and through integrated bricks and mortar service centres in six communities across BC. Each Foundry location is associated with a health authority that holds a funding agreement with MoH.*

Providence Healthcare: *Foundry involves many partnerships across BC. The Foundry Central Office is a program within Providence Health Care that leads the provincial initiative and supports the development of local Foundry centres. Each Foundry centre is operated by a lead agency that brings together local partners, service providers, young people and caregivers.*

BC Children's Hospital (BCCH): *A branch society of PHSA. Foundry's online platform, foundrybc.ca, is powered and supported by BC Children's Hospital. In partnership with BCCH, Foundry Online will build out its vision for eFoundry. BC Children's Hospital created the PIA for the foundrybc.ca/.*

BC Emergency Health Services (BCEHS) Critical Incident Stress (CIS) Program*: Unit within PHSA that supports BCEHS employees and their family e.g., paramedics and dispatchers, dealing with mild to moderate occupational stress related injuries, substance use issues, and returning to work from leave.*

Provincial Health Services Authority (PHSA): *PHSA provides province-wide specialized health services through its services and programs. Through BC Emergency Health Services, PHSA oversees the BC Ambulance Service and Patient Transfer Network.*

First Nations Health Authority (FNHA): *The First Nations Health Authority is a health service delivery organization responsible for administering a variety of health programs and service for First Nations people living in BC. In 2013, the FNHA assumed this role from Health Canada's First Nations Inuit Health Branch, Pacific Region. The project will seek guidance from the FNHA on how best to engage and work with rural and remote and First Nations youth and paramedic/dispatcher populations.*

Ministry of Health Primary and Community Care and Health Sector IM/IT: *MoH is participating on this project through a tripartite governance executive sponsorship through the Primary and*

Community Care Mental Health Substance Use program area and Health Sector IM/IT to oversee the execution of this project.

***Ministry of Mental Health and Addictions (MMHA)**: Organization responsible for setting provincial mental health substance use strategic direction and to implement government's commitment to transform the mental health and addictions system. MMHA is participating on this project through a tripartite governance executive sponsorship to the project director role.*

***TELUS:** TELUS is a vendor and provides resources through the SIF to perform work & services on behalf of the Province and Partners related to this initiative.*

[1] Telus (Telecommunications Service Master Agreement) https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/about-the-bc-government/strategic-partnerships/contract-administration-administrator-s-office/sra.pdf

2. Scope of this PIA

The scope of this PIA is to outline the Ministry of Health and Ministry of Mental Health and Addictions involvement in the MHSU Virtual Clinic project and the relationship between all participating parties.

If the scope of this project changes and the MoH becomes involved in the collection, use or disclosure of personal information a PIA initiative update will be completed.

3. Related Privacy Impact Assessments

Privacy Impact Assessments will be completed through Providence Health and PHSA that will assess the collection, use and disclosure of personal information in relation to both Virtual Clinics.

Foundry: Janet Scott, Providence Health (JScott@providencehealth.bc.ca)
Foundry Online/BC Children's Hospital Privacy: Privacy: Dawn Lake, Corporate Director, Information, Access and Privacy with PHSA.

4. Elements of Information or Data

The Ministry of Health will not be collecting, using or disclosing any personal information as part of this initiative. The Ministry will be supporting the project from a project management perspective and supporting the initiative financially through the SIF.

The MoH may receive aggregate reports on usage/uptake and effectiveness of the virtual clinic. These reports will not include personal information The MoH will not have custody or control of the personal information being collected, used or disclosed as part of this initiative.

If personal information **is** involved in your initiative, please continue to the next page to complete your PIA.

If **no** personal information is involved, please submit Parts 1, 6, and 7 unsigned to PCT at pia.intake@gov.bc.ca. A privacy advisor will be assigned to your file and will guide you through the completion of your PIA.

Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Joann Berekoff, MPA		21 November 2018
Privacy Analyst Privacy, Compliance and Training Branch Ministry of Citizens' Services	Signature	Date
		Click here to enter a date.
Director or Manager Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services **(if Personal Information is involved in this initiative)**	Signature	Date

Part 7 – Program Area Comments and Signatures

Jane London Project Director	jane london Signature	Dec 14, 2018 Click here to enter a date. Date

A final copy of this PIA (with all applicable signatures and attachments) must be provided to PCT for its records to complete the process. PCT is the designated office of primary responsibility for PIAs under ARCS 293-60.

PCT will publish the ministry name, business contact details and a brief summary of the PIA to the Personal Information Directory (PID) as required by section 69(2) of FOIPPA. If you have any questions, please contact your privacy advisor at PCT or call the Privacy and Access Helpline at 250 356-1851.

Privacy Impact Assessment for
MHSU VC PIA

PIA#: HLTH20103 / **MoH#:** 2020-57

Part 1 – General

Name of Ministry:	Ministry of Health		
PIA Drafter:	Vinicius Cid, Privacy Analyst, DPSP		
Email:	Vinicius.cid@gov.bc.ca	Phone:	**778-974-4022**
Program Manager:	**Paul Payne, Patient Empowerment Portfolio Lead, DHSI**		
Email:	Paul.payne@gov.bc.ca	Phone:	**778-974-2685**

1. Description of the Initiative

This initiative is to develop a Mental Health Substance Use Virtual Clinic (MHSU VC) mobile application 'Shiftwell' to help support BC EHS employees with mild to moderate mental health and substance use challenges. The MHSU VC will form part of the BC Emergency Health Service (BCEHS), Critical Incident Stress Program (CIS) services.

The MHSU VC mobile application will augment the CIS program and enhance it by providing:

- Specially developed and relevant clinical content on topics such as mental health prevention and resilience and COVID-19 specific clinical content,
- A unique, powerful and secure method of sharing their information with family/counsellors or designates, and
- An interactive tool to link the shift schedule (platoon calendar) to activities and content that support wellness

The CIS Program supports employees of Provincial Health Services Authority, BC Paramedic First Responders dealing with occupational stress injuries. The program is a peer-to-peer responsive program where frontline providers (paramedics and dispatchers) can be connected with a peer or professional counsellor to receive support.

BCEHS established this program to address a number of challenges:

- Increasing number of occupational stress injury survivors who are injured but still working and requiring support.
- Increasing number of employees with accumulated occupational stress challenges.
- Increasing number of frontline providers not receiving the necessary support for mental health or substance use challenges.
- Lack of qualified, occupationally appropriate support counsellors available for Mental Health support in rural and remote locations.
- A growing need to supply tools and resources to BCEHS employees that focus on resilience building and prevention of occupational stress injuries and substance use disorders.

- The current model of intake for the CIS program is by telephone “activation” into the program.
- Lack of available curated preventative resilience tools and supports

Sample reasons for activations:

- Serious injury to patients
- Direct request for Counsellor
- Event involving children
- Direct request for CIS Peer
- Cumulative stress events
- Working on relatives or known patient
- Event with physical threat to staff safety
- Serious injury on the job
- Prolonged incident ending with loss
- Excessing media interest
- Suicide of colleague
- Line of duty death

BCEHS will have a customer support team to assist Shiftwell front-end users with their day-to-day operations. However, the Ministry of Health (MoH) will be providing back-end technical and development support to enable the app’s opertion. CGI and Freshworks have been contracted by the MoH to that end.

2. Scope of this PIA

This PIA covers the Ministry of Health’s technical support for the Shiftwell application through CGI and Freshworks.

The development of the app itself is not being assessed in this PIA, which is addressed by PHSA’s PIA.

3. Related Privacy Impact Assessments

CITZ20038 – Microsoft Azure Cloud Services (Corporate PIA)
HLTH20017-HDPI Phase 2

4. Elements of Information or Data

Employees using the application will be providing the following pieces of information:

- First and Last Name
- Email address (will be a BCEHS domain)
- Role
- Employment Status
- Age Range
- Primary Work Location
- Profile image
- Calendar and schedule information
- MyPlan information (goals, activities, achievements, personal health information, etc.)

The app only asks for Name and Email from employees; all other entries are optional.

IP addresses will also be collected in order to authenticate invalid login attempts and are saved as part of server request logs. Aggregate information about user activity in the application (e.g. download count, page views) will also be collected.

If personal information **is** involved in your initiative, please continue to the next page to complete your PIA.

If **no** personal information is involved, please submit Parts 1, 6, and 7 unsigned to PCT at pia.intake@gov.bc.ca. A privacy advisor will be assigned to your file and will guide you through the completion of your PIA.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

Employee data will be stored in Microsoft Azure servers, which are compliant with data residency legal requirements, and managed by TELUS under contract by PHSA.

CGI and Freshworks employees will only access PI from s.15 within Canada.

All storage and access of personal information (including backups) occurs within the secure networks/servers of the Ministry and/or health authorities, which are located within Microsoft Azure's Canadian region only.

Routing:
s.15 is being used for all access with the exception of the following (which will use internet traffic):

- users accessing only the portal (to retrieve aggregate analytical outputs or submit files supplementary to analysis activities)
- to launch a virtual desktop having access to analytical tools and de-identified data stores
- to access the SFTP site used for ingestion

All internet traffic sits behind the Azure s.15
s.15

Azure s.15
As an additional access control option detailed in the Corporate PIA, s.15 will be included with HDP's use of Azure to strengthen the transparency of access to data including s.15
s.15

6. Data-linking Initiative

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative. If so, you will need to comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	no
If you have answered "yes" to all three questions, please contact a PCT Privacy Advisor to discuss the requirements of a data-linking initiative.	□

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	no
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	□

8. Personal Information Flow Diagram and/or Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	BCEHS employees download, install and make use of the s.15 application, providing their information as requested. The information is stored in servers managed by TELUS (under contract by PHSA). Health shares custody of the information through the CGI and Freshworks contracts, whose personnel will be allowed to access the information under certain circumstances (see steps #2 and #3).	Direct Collection (by PHSA) Indirect Collection (by Health)	s.26(c), (e) (PHSA) s. 27 (b) [33.1 (p)(i)]
2.	CGI and Freshworks provide technical support for s.15 users. In the course of their work, they will have the ability to view PI stored in the application. This access will only occur when staffers need to conduct significant technical maintenance and repairs.	Use (by Health)	32(c) [33.1(p)(i)]
3.	CGI and Freshworks provide production operational support for the s.15 application. In the course of their work, they will have the ability to view and access PI stored in the application. This access will only occur when staffers need to make significant changes to the application or for extraordinary requests (e.g. subpoena).	Use (by Health)	32(c) [33.1(p)(i)]

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Employees could access personal information and use or disclose it for personal purposes	Only select s.15 will have permissions that enable them to view PI, and for strictly production management purposes. Their activities are audited and logged. BCEHS staff are not granted any purposeful access to information stored within Azure	Low	High
2.	Someone other than authorized staff accesses encryption keys	While encryption keys are stored in Azure's s.15 s.15 Azure admins will not have access to them. Only designated MoH s.15 in the s.15 group will have access to the keys.	Low	High
3.	Information provided by user in the app does not belong to its actual owner	A BCEHS employees will download the s.15 mobile app from Apple Store for iOS cell phones or from Google Play for Android cell phones. The user will obtain access by registering and setting up a s.15 app account. After they have accepted and agreed to the Terms of Use and Privacy Policy a s.15 is sent to the BCEHS employee using their @bcehs.ca email. The s.15 is entered in the app and this completes the registration and account set up process.	Low	High

10. Collection Notice

A collection notice is not needed as the PHSA has their own collection notice and the MoH is collecting information indirectly under s.27.1(b) for the purpose of MHSU-VC.

Part 3 – Security of Personal Information

If this PIA involves an information system, or if it is otherwise deemed necessary to do so, please consult with your Ministry Information Security Officer (MISO) when filling out this section. Your MISO will also be able to tell you whether you will need to complete a separate assessment called a Security Threat and Risk Assessment (STRA) for this initiative.

11. Please describe the physical security measures related to the initiative (if applicable).

Ministry of Health staff involved in the initiative abide to ordinary physical security measures such as keycard access to offices, locked workstations and cabinets, and security personnel on premises.

CGI uses similar security measures, additionally requiring visitors to check in through a single checkpoint and to always be accompanied, as well as requiring employees to store client documents in a Document Management System. Freshworks follows the same security protocols as CGI.

Azure datacentres are well protected, featuring needs-only access, physical security, steel-and-concrete perimeter fences, on-site security checkpoints and two-factor authentication.

12. Please describe the technical security measures related to the initiative (if applicable).

Only s.15 team (purposely limited) will have access to the encryption keys specifically for production operational support.

The CGI and Freshworks team is contracted to the Ministry of Health to provider Tier s and s support. Only Tier s support will have potential access to the Application data. They would not be evaluating or changing data information and do not have any intention of sharing the information with EHS or PHSA from these support calls.

If necessary, using the encryption keys, an approved limited number of people could access data in the App if necessary.

Encryption keys will be stored in Azure s.15

- No platform level administrator (i.e. Microsoft Azure admins) will have access to the keys
- Designated Ministry administrators will be given access so that keys can be revoked
- s.15 in the production operations groups will have access to manage the keys
- Production operations will be limited to a subset of s.15 who require elevated permissions strictly for production management. All activities and actions will be logged for audit compliance.

The steps to access the information stored in Azure is as follows:

1. Access request to s.15 for trusted CGI/Freshworks employee to access Azure
2. Approval from s.15 granted, now employee can access the production environment
3. Support Request comes through requiring data access. Approval must be provided by s.15 and s.15 manager

13. Does your branch rely on security policies other than the Information Security Policy?

Government Core Policy and Procedures Manual

Contact: Gwen Lock, Ministry Information and Security Officer; 778-974-2707

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

Viewing of PI is restricted to a few select s.15 who must access the information for operational purposes.

While encryption keys are stored in Azure's s.15 , Azure admins will not have access to them. Only designated MoH s.15 and s.15 in the operations group will have access to the keys.

15. Please describe how you track who has access to the personal information.

All activities and actions will be logged for audit compliance. Freshworks/CGI will send audit reports to MoH and PHSA as part of audit practices.

PHSA could provision access to the Application data because they are Global Administrators. Their activities and actions are likewise logged for audit compliance.

The following events have audit logs associated with each of them:

s.15

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

Freshworks and CGI's work may include updating and correcting personal information belonging to Shiftwell users through technical support. However, BCEHS employees are expected to update and correct their own personal information.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

No.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

N/A

19. If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

N/A

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No

22. Will a personal information bank (PIB) result from this initiative?

No

Please ensure Parts 6 and 7 are attached unsigned to your submitted PIA.

Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Joann Berekoff		2020-10-14
Privacy Analyst Privacy, Compliance and Training Branch Ministry of Citizens' Services	Signature	Date
Dwayne McCowan	Dwayne Mc	2020-10-16
Manager, Privacy Operations Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	Signature	Date

Part 7 – Program Area Comments and Signatures

Paul Payne	Paul Payne	November 4, 2020 Click here to enter a date.
Program Manager	Signature	Date
		Click here to enter a date.
Ministry Contact Responsible for Security (Signature not required unless MISO has been involved.)	Signature	Date
CBarclay		Click here to enter a date. November 9, 2020
Assistant Deputy Minister or Designate **(if Personal Information is involved in this initiative)**	Signature	Date
Zen Tharani		Click here to enter a date. Nov 6, 2020
Executive Director or equivalent **(if no Personal Information is involved in this initiative)**	Signature	Date

A final copy of this PIA (with all applicable signatures and attachments) must be provided to PCT for its records to complete the process. PCT is the designated office of primary responsibility for PIAs under ARCS 293-60.

PCT will publish the ministry name, business contact details and a brief summary of the PIA to the Personal Information Directory (PID) as required by section 69(2) of FOIPPA. If you **have** ***any questions, please contact your privacy advisor at PCT or call the Privacy and Access Helpline at 250 356-1851.***

Privacy Impact Assessment for
Virtual Physician Pathways
PIA#: HLTH20051 / MoH#: 2020-32

Part 1 – General

Name of Ministry:	Ministry of Health		
PIA Drafter:	Carrie Cameron		
Email:	Carrie.cameron@gov.bc.ca	Phone:	778 974-2711
Program Manager:	John Wightman (MOIS)		
Email:	John.wightman@gov.bc.ca	Phone:	250 812-8898
Program Manager:	Kim Treider (HLBC/HEiDi)		
Email:	Kim.treider@gov.bc.ca	Phone:	604 215-5110

1. Description of the Initiative

As part of BC's COVID-19 response, there is an expedited need to expand the ability to share clinical information across various providers (virtual physician network providers identified to assist in the COVID-19 response). HealthLink BC is implementing a virtual physician call taker support service called 'HealthLink BC Emergency iDocs in-aid' (HEiDi) and the Rural Coordination Centre of BC (RCCBC)/BC Emergency Medicine Network (BCEMN) is implementing a rural virtual physician network (peer-to-peer) to support care delivery through a 24/7 service that supports rural/remote patients and primary/emergency care practices (RUDi, ROSe, CHARLiE and MaBAL[1]). As of April 1st, the Ministry of Health (MoH) approved funds to proceed with accelerated deployment of a shared EMR (MOIS - Medical Office Information System) to facilitate these virtual physician pathways. In phase 1, HEiDi physicians will chart into MOIS and in phase 2, RUDi, ROSe, CHARLiE and MaBAL physicians/specialists will chart into MOIS. MOIS is wholly owned, operated and supported by Bright Health Solutions Society (aka Bright Health and formerly Applied Informatics for Health Society).

Virtual care networks backed by a shared electronic medical record (EMR) and workflow supports will significantly increase the capacity of the health system to keep patients out of hospital and protect in-person family practice and health authority community clinics from overload. Virtual physicians (vGPs) can document their assessment, use clinical functionality to support the encounter (e.g. lab and prescriptions) and electronically send their documentation to both the Provincial eHealth Viewer and other clinicians in the patient's care team.

A shared EMR for these providers is essential for the safe and effective delivery of continuity of care to patients in the event that a patient requires the assistance of virtual physician services more than once. Information is needed to make appropriately informed management decisions,

[1] RUDi (Rural Urgent Doctor in-aid) – Emergency medical physicians; ROSe (Rural Outreach Support) – Intensivist/critical care specialists; CHARLiE (Child Health Advice in Real Time Electronically) – pediatricians, pediatric emergency physicians, and pediatric intensivists; MaBAL (Maternity and Babies Advice Line) – family physicians with expertise in maternal and newborn care.

detect deterioration early on, schedule and conduct appropriate follow-up over a period of time, and conduct safe handover of patients to their own primary care provider or team. This is particularly relevant in the context of the current COVID-19 pandemic, where a surge in demand for urgent clinical assessment is anticipated to overload existing family practice and community health authority services. Should this occur, a capacity to triage and manage potentially large numbers of patients through these two virtual services would be of significant benefit in reducing load on these primary care services and facilitating timely access to care.

In addition, a capacity for physicians to deliver intensive care in rural communities will likely be essential, and virtual support from intensive care specialists in urban areas will be a key enabler. This will be much more effective if the attending specialist has access to a shared electronic record containing both the patient's progress over time and the previous assessments of all physicians providing advice in the management of these very sick patients.

Concurrently, First Nations Health Authority (FNHA) are planning a "doctor of the day" program to provide virtual care to First Nations communities across the province. In this service, which also incorporates a shared EMR, care will be provided by many of the same physicians as will be providing care in the HealthLink BC and RCCBC/BCEMN virtual care services. Because of this, there is an opportunity for synergy by implementing a shared EMR for HealthLink BC and RCCBC/BCEMN that is identical in type and configuration to the FNHA shared EMR, enabling physicians to move easily between the two EMRs depending on which patient population they are serving, and enabling the HealthLink BC service to more effectively assist with meeting First Nations medical needs at times of high demand. FNHA's virtual solution is out of scope of this PIA as FNHA encounters will not be entered into MOIS and FNHA has completed a PIA for their own process.

2. Scope of this PIA

This PIA covers the collection of personal information by the HEiDi vGP from the patient and the encounter recorded for those patients by the HLBC Registered Nursing team, that are entered into the MOIS shared EMR by the vMOA (virtual medical office assistant). This information will be used by the patient's current vGP and may be accessed by any subsequent vGPs (and their vMOAs) providing virtual care and to the patient's regular GP, lab services, COVID testing site, etc. to provide ongoing care to that patient. Of note is that HEiDi physicians are contracted by MoH and are therefore covered under FOIPPA.

This PIA also covers the charting into the MOIS EMR by the RUDi/ROSe/CHARLiE/MaBAL physicians and the sharing (peer-to-peer) of patient personal information via the EMR.

The data flows into CDX and CareConnect and back to the calling physician by fax are out of scope of this PIA and are being assessed separately.

The virtual technology used for patient interactions (i.e. Zoom for Healthcare) is out of scope of this PIA and is being assessed separately.

3. Related Privacy Impact Assessments

CDX Project PIA – owned by IHA
Care Connect PIA Update – owned by PHSA
Zoom for HealthCare – owned by PHSA (in progress)
HLTH17043 – HLBC KDR (Knowledgebase, Decision Support and Client Record)

4. Elements of Information or Data

Patient Health information including PHN, diagnoses, medications, lab results, radiology results, and any other information required to create a patient profile.

Part 2 – Protection of Personal Information

5. Storage and Access Outside of Canada

Storage:
MOIS Cloud (including backups) is hosted at the Azure Canada Central data centre in virtual machines (VMs). Canada Centre East is used as a disaster recovery site. MOIS Cloud is integrated with Excelleris, CIX, CDX, Teleplan and Health Data Coalition systems (whose systems are out of scope of this PIA), which are all hosted entirely in Canada.

HEiDi records are stored within the BC Government's secure network and within the MOIS Cloud, which are located within Canada only.

Access:
MOIS Cloud, (which is wholly owned and operated by Bright Health, and all its parent companies are Canadian. Bright Health's entire infrastructure is on VMs that are administered uniquely by experienced, Canada-based, security-vetted, privacy-trained, full-time Bright Health employees who are subject to strong privacy and security policies.

All Bright Health infrastructure through which Personal Health Information (PHI) is accessible is implemented using VMs that are administered uniquely meaning that all access points to the VM are through MOIS/Bright Health and that Microsoft cannot access.

s.15

s.15

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative. If so, you will need to comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	N/A
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	N/A
If you have answered "yes" to all three questions, please contact a PCT Privacy Advisor to discuss the requirements of a data-linking initiative.	

7. **Common or Integrated Program or Activity***

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.

1. This initiative involves a program or activity that provides a service (or services);	yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	yes
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

8. Personal Information Flow Diagram and/or Personal Information Flow Table

s.15

Personal Information Flow Table			
	Description/Purpose – 811 Call Centre/HEiDi Physicians	**Type**	**FOIPPA Authority**
1.	Patient contacts 811 HLBC and is triaged to an HLBC nurse who interviews the patient, records information into KDR	Collection	26(c)
2.	Nurse passes call to vMOA to export records to PDF, upload to MOIS, and arrange call with vGP, adding patient to the day sheet	Use	32(a)
3.	Medical information is collected virtually from the patient by the vGP – encounter note and CV19 assessment (if required)	Collection	26(c)
4.	vMOA completes the patient chart with any new info from the encounter notes	Use	32(a)
5.	vMOA sends patient documents to Most Responsible Physician (MRP) or another GP (if	Disclosure	33.2(a)

	patient is attached to a community GP) as per vGP instructions*		
6.	If COVID-19 related and patient is symptomatic, the vGP or vMOA will provide advance notice to the COVID testing site that a patient is being directed there	Disclosure	33.2(a)
7.	Disclosure to CareConnect provincial repository via CDX, viewable by other CareConnect-enabled physicians and health practitioners (future state)	Disclosure Use – out of scope	33.2(a)
8.	If the patient sees a different physician, the vMOA or vGP will access MOIS to provide ongoing care and enter additional medical information into the MOIS (as per above)	Use	32(a)
9.	Bright Health may require temporary access to personal information in order to provide technical support (e.g. troubleshooting or routine maintenance). This access to personal information would only be from within Canada by authorized Bright Health personnel (no Microsoft access).	Disclosure	33.1(1)(p)

*Information may be sent by SRFax, an electronic fax solution contracted by MOIS. The security of the fax solution will be assessed separately.

On August 27, 2020, the MOIS EMR, also known as the Provincial EMR (P-EMR) was designated as a Health Information Bank under the eHealth Act. This allows for the indirect collection of patient personal information into the P-EMR by Rural/Remote (RUDi, ROSe, CHARLiE, MaBAL) physicians.

Personal Information Flow Table				
	Description/Purpose – Rural/Remote (R/R) Primary Care Providers	**Type**	**FOIPPA Authority**	**Other Authority**
1.	Patient contacts R/R physician on call – by video or phone	Out of Scope	-	-

2.	vGP responds to request from the rural physician and creates a patient chart in MOIS based on patient demographics	Indirect Collection
		Use
			26(c), 27(1)(a)((iii)
			32(a)
				Designation Order (M310-2020)

3.	vGP creates encounter note from within the newly created patient chart	Use	32(a)	Designation Order (M310-2020)
4.	vGP completes the patient chart	Use	32(a)	Designation Order (M310-2020)
5.	If lab orders/imaging req reports received, they are added to vGPs primary location and MOIS	Indirect collection	26(c), 27(1)(a)(iii)	P-EMR Designation Order (M310-2020)
6.	vGP distributes patient documents as needed to MRP and/or CareConnect (future state).	Disclosure	33.2(a), 33.1(1)(c)	Designation Order (M310-2020) – *eHealth Act* s.14
7.	If the patient sees a different physician, the vGP will access MOIS to provide ongoing care and enter additional medical information into MOIS (as per above)	Use	32(a)	Designation Order (M310-2020)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Someone not part of a patient's direct care could access PI on the shared EMR	Implementation of data segregation via pre-established, role-based privileges (i.e. security groups or data partitioning); therefore, providers do not have access to the same information.	Medium	High
2.	Information is entered into the wrong patient's EMR	Implementation of identification verification procedures and Information Incident Management Policy.	Low	High
3.	Inherent risk with cloud-based technology, including	Cloud Security Schedule and Cloud Privacy Protection Schedules have been sent to the	Medium	High

	storage, access and security of personal information as well as proper flow-through of requirements from government to service provider.	vendor for inclusion within the contract. Vendor will be required to adhere to these schedules as per the agreement. In addition, these risks are mitigated through the use of s.15		
4.	There is a risk of unauthorized access to personal information outside of Canada	MOIS' entire infrastructure is administered by Canadian based Bright Health employees who are subject to privacy and security policies (and bound by contract with the Province). *Bright Health has many layers of technical measures in place to protect against such unauthorized access. The risk of access by out of country Microsoft personnel is mitigated* s.15 s.15 The data is stored in Canada. Access to data at the infrastructure level is protected through the use of s.15 s.15		

10. Collection Notice

HealthLink

When an individual calls 811, they will hear the following pre-recorded message:

"Welcome to HealthLink BC. If you require any emergency service or if someone in your care has chest pains, difficulty breathing or severe bleeding, call 911 now or the emergency number in your phone book. If this call is about a possible poisoning or exposure to a toxic substance call poison control now at 1-800 567 8911. Please note that calls are recorded for quality and training purposes. Personal information is collected under section 26 (c) of the Freedom of Information and Protection of Privacy Act for the purpose of providing, planning and evaluating health services. Please notify your HealthLink BC representative if you have questions regarding the collection of your personal information. A representative will be with you shortly."

The vMOA script is provided in the appendix.

RUDi/ROSe/CHARLiE/MaBAL

Information will be collected directly from the patient from the attending physician. The physicians will have their own existing process and authorities as to how information will be collected; their process is out of scope for this PIA.

The information collected by MOIS does not require a collection notice as per s.27(2) of FOIPPA since it is all collected indirectly.

Part 3 – Security of Personal Information

A Security Threat and Risk Assessment (S2020-15) is being completed for this initiative.

11. Please describe the physical security measures related to the initiative (if applicable).

HEiDi encounters are contained within restricted applications/folders (s.15 s.15 on the Ministry's secure network. The Ministry requires key card access to the building and any paper files will be in locked cabinets.

The MOIS Cloud EMR is a general purpose electronic medical records product. The user authentication method requirements for MOAs and Physicians are: s.15 s.15 Full details relating to system architecture can be found within the STRA.

12. Please describe the technical security measures related to the initiative (if applicable).

User access to the data is only through the application's business logic which enforces a role-based access control system. The data layer is isolated from the application layer with a

s.15

13. Does your branch rely on security policies other than the Information Security Policy?

Government Core Policy and Procedures Manual,

Contact: Gwen Lock, Ministry Information and Security Officer; 778-974-2707

Privacy, Security and Cloud schedules to be included in the GSA Contract

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

Access to personal information is based on the least privilege and need-to-know principles; within the MoH, the vGPs and vMOAs (as well as office manager, super user, and assistant office manager as needed), only a limited number of individuals will have access to the information needed to provide patient care. In addition, HLBC IT support may be required to troubleshoot problems and provide local on-site support before escalating to Bright Health s.15 technical support.

Bright Health has s.15 which are needed to maintain the system and s.15 are assigned to each person. All logons are logged. Only a few Bright Health employees have s.15 and only on a need basis. All access requires s.15

Bright Health currently provisions and revokes access to the HealthLink instance of MOIS based on instructions from HealthLink. Bright Health provisions an s.15 to a designated s.15 user for which s.15
s.15

MOIS has comprehensive, s.15
s.15

Limiting Microsoft Access:

All components of MOIS s.15 and the onus is entirely on Bright Health to manage them. There is no use of any application that Microsoft offers above the service layer on s.15 Microsoft personnel have no access, administrative or otherwise, to these s.15 they have no accounts, logins or user logins. As such, s.15
s.15

15. Please describe how you track who has access to the personal information.

vMOAs and vGPs will have to sign into the EMR using their s.15
s.15

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

Patient's can contact their physician or BC Medical Services to have their information updated.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

No, the virtual EMR does not use personal information to make decisions that directly affect an individual. The doctor's visit will, but that is out of scope of this PIA.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

N/A

19. If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

N/A

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No

22. Will a personal information bank (PIB) result from this initiative?

No

Part 6 - PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Joann Berekoff		16 October 2020
Privacy Analyst Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	Signature	Date
Dwayne McCowan	Dwayne MC	October 23, 2020
Manager, Privacy Operations Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	Signature	Date

Part 7 – Program Area Comments and Signatures

Leanne Thain		January 13, 2021
Program Manager (HSIMIT)	Signature	Date
Sandra Sundhu	SSundhu	October 29, 2020.
Program Manager (HLBC)	Signature	Date
Gwen Lock	Gwen Lock	2021-01-13
Ministry Contact Responsible for Security (Signature not required unless MISO has been involved.)	Signature	Date
Corrie Barclay	CBarclay	January 13, 2021
Assistant Deputy Minister or Designate **(HSIMIT)**	Signature	Date
Ted Patterson		October 29, 2020
Assistant Deputy Minister or Designate **(HLBC)**	Signature	Date

A final copy of this PIA (with all applicable signatures and attachments) must be provided to PCT for its records to complete the process. PCT is the designated office of primary responsibility for PIAs under ARCS 293-60.

PCT will publish the ministry name, business contact details and a brief summary of the PIA to the Personal Information Directory (PID) as required by section 69(2) of FOIPPA. If you have any questions, please contact your privacy advisor at PCT or call the Privacy and Access Helpline at 250 356-1851.

Appendix A – vMOA scripts

Current script read by vMOAs with addition for use of Zoom (scheduled for May 19th):

When we finish this call, I will disconnect, and the physician will be calling you back at this number (repeat number if necessary). When the physician calls you back, it will not indicate 8-1-1 on your call display. Rather it will show a Zoom call area code, such as 646, 212 or another North American area code or city.

While you are speaking with the physician, please be aware that they will be taking detailed notes, their calls are not recorded. The information the physician collects may be shared with your own doctor or nurse practitioner or another health professional in the community if the physician refers you for in-person care.

Before I disconnect, do you have any questions? (If no) – Thanks for calling 8-1-1, please be ready for the physician to contact you.

Zoom Chat (additional to call closing)
You will be receiving an email from HealthLinkBC momentarily that will provide instructions on how to prepare for your video assessment with the physician.

Please take a moment to read through the email and ensure you are able to access the zoom video chat. The instructions on how to do so are in the email.

When the physician connects with you, they will confirm the video is working well for you, and you are ready to begin an assessment. Please know that if you do have any technical challenges or if you change your mind regarding video with the physician, you can instead speak with the physician by phone.

Before I disconnect, do you have any questions? (If no) – Thanks for calling 8-1-1, please be refer to your email for next steps.

Recorded Announcements:

Initial call into 811 – HealthLink BC Disclaimer RAN
Welcome to HealthLink BC. If you require any emergency service or if someone in your care has chest pains, difficulty breathing or severe bleeding, call 911 now or the emergency number in your phone book. If this call is about a possible poisoning or exposure to a toxic substance call poison control now at 1-800 567 8911. Please note that calls are recorded for quality and training purposes. Personal information is collected under section 26 of the Freedom of Information and Protection of Privacy Act for the purpose of providing, planning and evaluating health services. Please notify your HealthLink BC representative if you have questions regarding the collection of your personal information. A representative will be with you shortly.

VMOA Agents Unavailable – played every 30 seconds
Thank you for holding. The next available Medical Office Assistant will assist with connecting you to a physician.

VMOA Agents Unavailable – played every 2.5 minutes
Thank you for continuing to hold. We are experiencing heavy call volumes at this time. If you choose to remain on the line, the next available Medical Office Assistant will assist with connecting you to a physician.

VMOA Agents Unavailable after 15 minutes
We apologise for the inconvenience. Due to high call volumes the Medical Office Assistant is unable to answer your call. Please hang up and seek medical care, as discussed with the nurse. Thank you for calling HealthLink BC.

No Agent in Service (EG: outside of business hours)
A Medical Office Assistant is not available to answer your call. Please hang up and seek medical care, as discussed with the nurse. Thank you for calling HealthLink BC.

Privacy Impact Assessment for Non-Ministry Public Bodies

Hospital at Home – HLTH21003

Why do I need to do a PIA?
Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA. Public bodies should contact the privacy office(r) for their public body to determine internal policies for review and sign-off of the PIA. Public bodies may submit PIAs to the Office of the Information and Privacy Commissioner for BC (OIPC) for review and comment.

If you have any questions about this PIA template or FOIPPA generally, you may contact the Office of the Chief Information Officer (OCIO) at the Privacy and Access Helpline (250 356-1851). Please see our PIA Guidelines for question-specific guidance on completing a PIA.

What if my initiative does not include personal information?
Public bodies still need to complete Part 1 of the PIA and submit it along with the signatures pages to their privacy office(r) even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

Part 1 – General

Name of Department/Branch:	Ministry of Health		
PIA Drafter:	Katherina Herman		
Email:	Katherina.Herman@gov.bc.ca	Phone:	**778 974-2705**
Program Manager:	**Leah Smith**		
Email:	Leah.Smith@gov.bc.ca	Phone:	**778 698-1340**

1. Description of the Initiative

The Hospital at Home (HaH) program is an innovative approach to providing acute care to patients in their own home. Patients eligible for hospital at home would be admitted to hospital and receive general hospital services while in their own home.[1] The severity of the condition and requirement for hospital admission differentiates hospital at home from other existing services such as community services and other approaches to virtual care. At times, it may be necessary for patients to return to the hospital for care, such as medical imaging, that cannot be provided at home. To

[1] General hospital services are defined in the Hospital Insurance Act Regulation 5.2. A condition for benefits is that the patient must be admitted as an in-patient by an appropriate healthcare provider. On recommendation of the healthcare provider this includes access to benefits such as, nursing care, drugs, laboratory and radiological procedures.

facilitate seamless access to all hospital services, HaH patients are considered admitted to the hospital with inpatient status.

Each HaH program will continue to have a physical space at the hospital. Some members of the interdisciplinary care team may be present at the hospital for portions of their shift carrying out activities such as providing preliminary assessments for admission, virtual care and monitoring. At other times, health care providers such as nurses and physicians will attend the person's home to provide in-person care. The specific mix of in-person, virtual care and monitoring will be determined by the patient's care needs.

Patients admitted to the HaH program are under the care of an appropriately qualified and privileged most responsible practitioner who is a member of the health authority's medical staff. The healthcare provider's responsibilities to the patient as set out in the Hospital Act, Hospital Insurance Act, Medical Staff Bylaws and Medical Staff Rules remain in place regardless of whether the services are provided within the hospital or through the hospital in a patient's home. Regulatory college standards, limits and conditions also continue to apply. HaH patients will also receive medically necessary nursing care. Drugs will be dispensed through a hospital pharmacy and costs will be absorbed by the hospital in line with the Hospital Insurance Act and Regulations.

Each HaH program will develop detailed eligibility criteria to guide patient admission to the program. The eligibility criteria will be reviewed by the Ministry of Health before implementation by the program. The admission criteria will ensure that each patient's acute care needs can be safely met at home. For example, to be admitted to hospital at home the patient must have a known diagnosis, be clinically stable and have an anticipated short-term need for acute care (i.e. under seven days). This will assist the care team to better anticipate and plan to meet the patient's needs.

Beginning in the fall of 2020, the Vancouver Island Health Authority (VIHA) will pilot the first HaH program at Victoria General Hospital with additional HaH programs to follow across the Health Authorities. VIHA will conduct a privacy impact assessment on their local deployment which will be appended to this Provincial PIA.

General Model

The HaH teams located across health authorities will include health care professionals such as physicians, nurses, administrative support, and allied health such as pharmacists. HaH will function as a ward of the hospital and patients will be registered as inpatients. The program will offer round-the-clock substitutive hospital care. HaH will operate under the governance of the provincial Hospital Act as well as the provincial Hospital Insurance Act with physicians receiving coverage from the Canadian Medical Protective Association.

At each site, the reach of hospital programs has evolved beyond the 'brick and mortar' environment with increasingly complex care being provided outside of the hospital walls. In this way, a hospital has extended beyond a brick and mortar facility to a not for profit institution focused on providing high quality care. The HaH program will be supported by an office or "hub" that is located in the hospital. These designated offices or hubs may include individual workstations, staff conferencing area, electronic patient tracker screens, an area to perform virtual visits and receive patient monitoring data and areas for medication and equipment storage. HaH will be based out of the relevant hospital or "parent" hospital and rely on the hospital facility and its institutional structures to allow for the provision of hospital services in the patient's home.

To ensure the provision of high-quality patient care, it is expected that quality and patient reviews will be carried out. Given the interconnected nature of the services provided both in and through the hospital, it is expected that some quality and safety reviews will rely on s. 51 of the Evidence Act and will be conducted by a committee/council approved by the hospital board of management. Information collected in the course of a s. 51 review is prohibited from unauthorized release.

2. Scope of this PIA

The purpose of this PIA is to provide a high-level overview and assessment of the HaH program which includes the provincial direction of the program including general collection, use and disclosure of personal information required for the delivery, management, operation, and evaluation of the program.

Each health authority deploying the HaH program will conduct an assessment of local operations which will include any unique activities and their associated risks. As a result, the following are considered out of the scope of this Provincial PIA: local processes; the additional collection, use or disclosure of personal information; and the use of specific technologies for monitoring and providing virtual care. Technology will include health record management, video or phone conferencing, capabilities for remote consultations and team meetings, and remote patient monitoring technology.

Local level assessments can be found appended to this PIA (please see attached Schedule).

<u>Overview</u>

The scope of the HaH program generally accepted processes includes:

- *Health authority patient eligibility and suitability assessment to participate in the HaH program ending with patient discharge from the HaH program*

- *Patient information collected during the HaH program enrollment period*
- *Reporting of HaH program data including adverse event data to the Ministry of Health*

Out of Scope

- *Health authority handling of patient information for HaH technical equipment management procedures*
- *Handling of patient information for accuracy, correction and retention*
- *Secondary use of personal information for research*
- *Review of the technical end to end processes and workflows for collecting, using and disclosing personal information for the purposes of delivering the HaH program including any secondary use of data for research*
- *Specific security device and equipment management*
- *Organization-specific workflows and procedures that may deviate from the workflows or procedures described in this PIA or that may already be addressed in separate PIAs completed by the health authorities. These organization-specific workflows will be addressed in PIAs by the health authorities included in the appended schedules. Examples of exclusions are as follows:*
    - *Physical security controls in place on workstations where patient information is accessed by health authority users*
    - *Health authority specific referral and intake procedures*
    - *Process for managing the use of the document upload tools*
    - *Changes to equipment installation or retrieval procedures due to health authority-specific roles and responsibilities and operational requirements*
    - *Disclosure of personal information for research purposes under FOIPPA s.35*
    - *Monitoring compliance of health care providers (e.g. reporting on duration of virtual visits)*

3. Related Privacy Impact Assessments

There are no related PIAs to the HaH program. Please see the attached Schedules for further information on local HaH operations.

Vancouver Island Health Authority will employ the use of Telus Home Health Monitoring to support the HaH program, as such, the 2018 BC MoH HHM Master PIA may be referenced including the AWS Transition PIA and STRA.

4. Elements of Information or Data

Although not an exhaustive list, the following is a sample of the personal information that will be collected, used and or disclosed for the purpose of the HaH program:

Purpose	Individual	Possible Data Elements
Registration/Intake	*Patient*	*Admission date will include demographic information* *Patient name* *PHN and any unique identifier (medical record number, driver's license number, government-issued ID number)* *Gender* *Language* *Patient's home address* *Patient phone number* *Patient consent/agreement* *Patient intake information (date of birth)*
	Caregiver	*Name* *Address* *Telephone/email* *Relationship with patient* *Consent Agreement*

System Reporting (e.g. DAD)	*Patient*	*Personal Health Number* *Date of Birth* *Gender* *Client Health Authority* *Admission date* *Discharge date* *HaH-specific codes that indicate that it is specifically a HaH occurrence*
Clinical Monitoring Devices *Remote Patient Monitoring*		*Patient biometric data including weight, blood pressure, pulse, glucose, pedometer, oxygen saturation, heart rate* *Standardized Clinical Assessment Tools and Surveys, including:* *General Anxiety Disorder (GAD -7)* *Patient Health Questionnaire (PHQ-9)* *Pain Disability Index (PDI)* *Virtual device information*
Virtual Care	*Patient* *Healthcare provider*	*Image and likeness, voice* *Virtual device information*
On-Site Visits	*Patient & Caregiver*	*Patient medical information such as diagnosis, treatment, diagnostic results (e.g. labs and imaging) care notes (allergies), medications, hospital admissions, cognitive status, mobility issues, sexual health, immunization status,*

		lifestyle information, procedural history, reason for visit, violence alerts and infectious disease precautions. Medical specialist diagnosis (e.g. mental health and substance abuse information). *Please see appended schedules for a more comprehensive list of potential data collected.*
	Healthcare provider	*Healthcare provider name* *Practice/Speciality - Physician Specialty (Dermatology, Haematology & Oncology, General Internal Medicine, Emergency Medicine, Gastroenterology, Immunology, Trauma, Intensivist).* *Along with professional opinion, medical record notes may include personal opinion.*
Reports	*Patient* *Healthcare provider*	*Records shared with professional health care team such as GP or specialists may include any of the above listed data. elements.* *Health authority reports shared with MoH may include the following data:* • *Date of referral* • *Medical Record Number* • *Referring physician* • *Acceptance or decline to HaH* • *Reason for decline* • *Patient deemed ineligible*

		- *Patient repatriation into hospital* - *Length of stay* *Health authorities may also keep incident logs detailing issues with workflows, patient or staff safety and similar details.* *Health authorities are to provide reports to the Ministry of Health including numbers on how many patients are accessing HaH.*
Patient Safety & Learning System	*Patient* *Healthcare provider* *Caregiver*	*BCPSLS source of incidents reported which includes adverse event, negative outcomes, near miss, hazards.*
Evaluation	*Patient* *Healthcare provider* *Caregiver*	*Program evaluations may include patient level data such as patient and caregiver satisfaction, professional opinions and care reports. This may also include evaluation processes developed by the health authorities to gather patient and caregiver feedback through HaH participant engagement.* *Aggregate statistics such as time in care, hospital visits and discharge data will also be created and shared between the Ministry of Health and health authorities.* *Health authorities will provide adverse event reports to the Ministry of Health. Adverse event data will not identify individuals but provide information about the event as well as any medical information. Reports may reidentify individuals due to the mosaic effect.*

Transport	*BC Ambulance Service* *Medivan* *Taxi*	*Ambulance services will obtain the necessary personal information to provide care to patients (biometrics, health events, allergies and medication information if appropriate). Other transportation services such as Medivan and taxi services will only collect patient name and patient address.*

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 to your privacy office(r). They will guide you through the completion of your PIA.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

All personal information will be securely accessed and stored within Canada. Please see appended health authority schedules for details on any instances where data may be stored or accessed outside of Canada.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	no
If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.	

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	yes
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

8. Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	*Health authority collects personal information to determine patient's eligibility for the HaH program.* *If patient is eligible, then patient consent to the terms and conditions of the HaH program (please see appended schedules for more information).* **Please see appended health authority schedules for any additional authorities for specific activities such as indirect collection of PI from community healthcare providers.*	*Collection*	*s. 26(c)*

2.	*Healthcare providers collect personal information from patients to provide care (virtual and on-site, please see appended schedules for details on the collection, use and disclosure of personal information by platform vendors).*	*Collection*	*s. 26(c)*
3.	*Patient provides information directly to transportation services or the health authority provides the PI on behalf of the patient for the purpose of transporting the patient to or from the hospital or clinic.*	*HA Disclosure* *Public Transport* *Collection & Indirect* *Use* *Private Transport* *Collection & Indirect* *Use*	*s. 33.2(a)* *s. 27(1)(a)(i), (a.1)* *s. 26(c)* *s. 32(a)* *PIPA* *s. 8(1)* *s. 12(1)(a), (b)* *s. 14* *s. 15(a), (b)*
4.	*Health authority collects patient and healthcare provider personal information to manage and evaluate the HaH program.* *Research is considered out of the scope of this PIA.*	*Collection* *Use*	*s. 26(e)* *s. 32(a)*
5.	*Health authority discloses administrative, clinical, demographic information on hospital discharges (deaths, sign-outs and transfers) for inclusion in the Discharge Abstract Database which is also made available to the Canadian Institute for Health Information (CIHI).* *Health authority also discloses adverse event data to MoH for reporting and investigation*	*Disclosure*	*s. 33.2(a)*
6.	*MoH collects adverse event data from health authority involved.*	*Collection*	*s. 26(c), (e)*

	MoH uses adverse event data to assess program safety. *MoH shares adverse event data and program outcomes with health authorities across the province to improve program delivery and inform best practices.*	*Use* *Disclosure*	*s. 27(1)(b) [as per 33.2(a)]* *s. 32(a)* *s. 33.2(a), 33.2(l)*
7.	*Health authorities disclose patient financial information to MoH. This disclosure may include other third parties such as WCB, ICBC or private insurers.* *MoH collects patient financial information for the purposes of administering and managing MSP.*	*Disclosure* *Collection* *Use* *Disclosure*	*s. 33.2(a)* *26(c) [s. 5(e) of the Medicare Protection Act]* *32(a)* *33.2(a) [s. 49(2)(a) of the Medicare Protection Act and s.4(e) of the E-Health Act]*
8.	*Health authorities disclose de-identified HaH program information to MoH.*	*No PI*	*N/A*
9.	*MoH collects aggregate de-identified program data from health authorities for evaluation and reporting purposes.*	*No PI*	*N/A*

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*Employees could access personal information and use or disclose it for personal purposes*	*Health Authority contractual terms, privacy and security training.* *Auditing programs depending on health authority, please see*	*Low*	*High*

		attached PIAs for more information.		
2.	*Patient information may be compromised when healthcare provider is travelling between locations*	*Healthcare provider will employ reasonable security including device encryption, secure storage and supervision of documents. Please see security section for additional information.* *Specific policies and processes developed by health authorities will be employed for the secure management of patient information while in transit.*	*Low*	*High*
3.	*Patient personal information may be compromised during virtual visits*	*Healthcare providers will ensure there is privacy and verify patient identity prior to providing care and adhere to health authority privacy practices and procedures for conducting virtual care visits.* *Please see appended schedules for security details.*	*Medium*	*High*
4.	*Patient information may be compromised in the Health Authority's information system*	*Appropriate security including encryption, firewalls role based and password protected access to only those who "need to know". Please see the specific security details outlined the appended health authority schedules.*	*Low*	*High*
5.	*The healthcare provider may unintentionally collect the personal information of non-HaH patients (family, friends etc.)*	*The healthcare provider will ensure there is privacy in the residence prior to treating patient.* *Should it be necessary to collect non-patient personal information for the purposes of delivering care*	*Medium*	*Medium*

		or documenting care that was provided, the healthcare provider will request permission and remove any identifying information where possible.		
6.	*Patient may collect information about the healthcare providers when receiving care in their home*	*Patient will agree to the terms and conditions of the program requiring them to avoid collecting their healthcare provider's personal information e.g. via video surveillance, audio recording without the healthcare provider's consent.* *The healthcare provider will adhere to the specific policies and practices of their respective health authority. Please see appended health authority schedules for additional information.*	*Low*	*High*
7.	*s. 51 of the Evidence Act may be deemed inapplicable resulting in the potential disclosure of personal information included in the Patient Safety Learning System.*	*HaH program governance is such that the physical hospital is the hub from which services are delivered to patients in their homes resulting in a strong rationale for the applicability of s. 51.*	*Medium*	*Medium*
8.	*Adverse event reports may identify individuals and include sensitive personal information*	*The identity of individuals will be excluded from reports along with any identifiers. However, due to the mosaic effect (small cell size or media coverage), it may be difficult to completely deidentify the report. As a result, adverse event reports will be treated as personal information and subject to the necessary security*	*Low*	*High*

		protections to prevent unauthorized access (please technical security for more details).		

10. Collection Notice

Please see appended Schedules for Collection Notices, Consent Notices and Terms and Conditions Agreements.

Part 3 – Security of Personal Information

11. **Please describe the physical security measures related to the initiative (if applicable).**

All paper records will be stored in locked cabinets. Paper records created during off site visits will be kept with the healthcare provider for safekeeping and securely attached to a folder. A secure case will be used to carry files such as a locked briefcase or sealed box.

Documents will not be opened or reviewed while in transit and will not be left unattended. Devices and equipment will be under the care of the healthcare provider at all times or locked away securely if this is not possible.

Healthcare provider devices such as laptops will be securely locked away or kept on the healthcare provider while at a patient's residence. During virtual visits, healthcare providers will ensure they and the patient have privacy prior to providing care.

Any specimens that are collected during on-site visits will be stored in lab approved transport containers and managed according to health authority procedures and policies to ensure they are secure.

Healthcare providers will only bring necessary records to offsite visits and adhere to their respective health authority's policies and procedures.

12. Please describe the technical security measures related to the initiative (if applicable).

All personal information will be protected using appropriate security measures that are commensurate with the sensitivity of the data. This will include the use of firewalls, encryption, password protecting devices and documents.

Off-site patient care and the documenting of such care will be done in a private setting to prevent an unauthorized disclosure of personal information.

HaH devices (both healthcare provider and patient) will automatically lock after a set time of idleness where applicable. All HaH devices will be up to date with virus software and firewalls and adhere to the required security standards developed by the respective health authority.

Encrypted emails with password protected documents will be used to send adverse event data between the health authorities and the Ministry of Health program area. The Ministry of Health's program executive director and director will receive the emails and only those team members who need to know the adverse event data will have access to the report which will be stored on a restricted LAN.

13. Does your branch/department rely on any security policies?

Each health authority has security policies that govern the use of systems and management of confidential records. Please see the appended schedules for more information.

The Ministry of Health Information Privacy Policy.

Government Information Security Policy and Government Core Policy and Procedures Manual.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

Access controls for devices and virtual technology will only be accessible to those providing patient care.

Access to patient health records is limited to those who have credentialed access to systems and accounts on devices. Audit logging tracks access to electronic records which monitor use. Additionally, each system has audit capabilities to track access and assist in identifying unauthorized access. Please see attached schedules for more information.

For specific details on the prevention of unauthorized changes, please see the attached schedules.

15. Please describe how you track who has access to the personal information.

The Health Authorities will regularly audit access to devices and systems used to collect patient information.

Each health authority has a process for the management of patient information while off-site, this includes policies for tracking access to personal information. Please see attached schedules for more information.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. **How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?**

    Patient information can be updated by the healthcare provider. Each health authority has established processes for updating or correcting patient information into their HaH-related devices or systems.

17. **Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.**

    Yes, personal information collected will be used to make healthcare decisions about the patient. Personal information collected about healthcare providers may be used to make changes to the healthcare providers' work-related tasks, accountabilities including any disciplinary action.

18. **If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

    Healthcare providers will verify that a patient's personal information is accurate and complete during documentation. This information may be reviewed in follow-up visits to confirm that information has not changed. Individuals may request a correction of personal information with the health authority and corrections or annotations are completed in accordance with health authority policies and FOIPPA.

    The health authorities will verify the healthcare provider's information to ensure accuracy. This information will be reviewed periodically as per the health authorities' policies and procedures.

    Adverse event data received by the MoH will contain opinions and personal accounts of adverse events. As a result, such information may be deemed incomplete or partial. While the collection of such data is undertaken by the health authority who will endeavour to capture accurate information, the MoH will follow-up on any discrepancies that may arise.

19. **If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?**

    Each health authority will employ the appropriate record retention schedules. Patient records created in hospitals are managed according to the Hospital Act Regulations.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact your privacy office(r).	

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

Any secondary use of HaH data will be addressed by the individual health authorities who are conducting the research or disclosing the information to researchers. Please see the appended schedules for additional information.

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact your privacy office(r).	

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.

A personal information bank will be created within each HaH program when data is entered into the health authorities' respective electronic health records and when there is a disclosure to any subsequent provincial systems.

Please ensure Parts 6 and 7 are attached to your submitted PIA.

Part 6 – Privacy Office(r) Comments

This PIA is based on a review of the material provided to the Privacy Office(r) as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA Update and submit it to Privacy Office(r).

Privacy Compliance and Training Branch (PCT) of BC Ministry of Citizen's Services:

While this PIA contemplates the entirety of the Hospital at Home Program, PCT recognizes the scope of the Ministry of Health's (MoH) involvement is to provide program funding, eligibility criteria, adverse event data and program outcomes to Health Authorities as well as collect de-identified program data, adverse event data and patient financial information. Within this scope, PCT agrees that the Ministry's collection, use and disclosure of personal information is authorized under FOIPPA as well as meeting all legal requirements. PCT is not providing review and comment on the legal authorities or requirements of regional or provincial health authorities.

PCT Signatures

This PIA is based on a review of the material provided to PCT as of the date below.

PCT Privacy Advisor	PCT Director
Cole Lance	Quinn Fletcher
2021-01-26	2021-01-27

Part 7 – Program Area Signatures

Leah Smith

Program/Department Manager Signature Date

Head of Public Body, or designate Signature Date

A final copy of this PIA (with all signatures) must be kept on record.

If you have any questions, please contact your public body's privacy office(r) or call the OCIO's Privacy and Access Helpline at 250 356-1851.

Privacy Officer/Privacy Office Representative Signature Date

<u>Appendix A – Vancouver Island Health Authority PIA</u>