



# Privacy Impact Assessment for *Zoom usage in MoH* PIA#: HLTH19050 / MoH#: 2019-11

## **Part 1 – General**

Name of Ministry:	Ministry of Health		
PIA Drafter:	Katherina Herman, Sr. Privacy Analyst, HIPSL		
Email:	<a href="mailto:Katherina.herman@gov.bc.ca">Katherina.herman@gov.bc.ca</a>	Phone:	778 974-2705
Program Manager:	Don Stewart		
Email:	<a href="mailto:Don.Stewart@gov.bc.ca">Don.Stewart@gov.bc.ca</a>	Phone:	250 952-2307

### **1. Description of the Initiative**

*The Ministry of Health seeks to employ the use of Zoom, a web-based conferencing tool. Zoom may be used in a variety of ways by business areas to assist in their daily activities or initiatives by enabling multiple parties to conference from various locations and support effective project and time management. For example, Zoom may be utilized when conducting meetings, focus groups or interviews with contractors, partners, and stakeholders outside of government or with those in remote locations; thereby increasing access, reducing resource expenditures and saving time.*

### **2. Scope of this PIA**

*This PIA will not address the privacy implications of the projects, activities or programs which will utilize the use of Zoom technology. Rather, the overarching PIA will address the Zoom technology which may collect, store or disclose personal information as a result of its inherent qualities (video, and audio recording capabilities). The purpose of employing the use of Zoom is to enhance communication with external stakeholders for purposes of project management and/or the execution of employee duties.*

### **3. Related Privacy Impact Assessments**

- *Ministry of Children and Family Development completed an overarching ministry PIA on Zoom (PIA # CFD18023) in March of 2019.*
- *MoH#2019-13 recently submitted for review*
- *MoH STRA S2019-20*

### **4. Elements of Information or Data**

*Personal information or business confidential information may be collected, used or disclosed through the use of Zoom. Additionally, documentation and other materials may be shared and edited through Zoom. The IP addresses of conference participants, device identifiers and contact*



# Privacy Impact Assessment for

## Zoom usage in MoH

PIA#: HLTH19050 / MoH#: 2019-11

---

information such as name and email address may be collected during the registration process to access Zoom services. Zoom automatically collects information regarding usage of the service, actions taken, date and time, frequency, duration, quantity, network connectivity and performance information related to logins, clicks, messages, contacts, content shared, calls, use of video and screen sharing, meetings, cloud recording and other information.

Zoom and third-party service providers and advertising partners such as Google Ads and Google Analytics automatically track information (e.g. IP, browser type, internet service provider, files viewed on site etc.) using cookies. Users can control the use of cookies on the individual browser by going to the Zoom homepage and selecting the "Cookie Preferences" link.

Zoom is a cloud-based platform, with SSL and AES 256-bit encryptions. Zoom only stores basic account information, and unless the option is selected to record meetings to the Zoom cloud, Zoom does not record or store any content. The Zoom mobile app will not be used. Content or functionality that is hosted by a third party and accessed via Zoom will not be used.

A Ministry wide STRA has been completed by the Ministry of Health (S2019-20) and has also been completed in the Ministry of Children and Family Development which did not uncover any significant security challenges.

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](mailto: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**

Zoom is a US based company with servers located in the United States. However, Zoom also has data centres in Toronto and Vancouver enabling all live meeting data and traffic to reside in Canada.

Zoom and third-parties such as Google Analytics and Google Ads perform analytics on data such as login usage trend, service delivery, as well as conducts passive data collection through the use of cookies. This information may include personal IP addresses if Zoom participants use personal devices. Such data may be accessed or stored outside of Canada and is included in the Collection Notification.



# Privacy Impact Assessment for

## *Zoom usage in MoH*

PIA#: HLTH19050 / MoH#: 2019-11

---

*Any meeting recordings will only be stored on password protected LAN located on government servers. Finally, while geolocation services are available in Zoom, they will not be employed by the MoH.*

### 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
<b>If you have answered "yes" to all three questions, please contact a PCT Privacy Advisor to discuss the requirements of a data-linking initiative.</b>	



# Privacy Impact Assessment for Zoom usage in MoH

PIA#: HLTH19050 / MoH#: 2019-11

## 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.	Licence holder business information is provided to Zoom.	No PI	N/A
2.	Audio and video of employees/contractors and stakeholders are streamed over Zoom.	Collection Use Disclosure	26(c) 32(a) 33.2(a)
3.	Documents containing personal information may be shared or edited over Zoom.	Collection Use Disclosure	26(c) 32(a) 33.2(a)
4.	Disclosure of IP addresses for participants using personal computers or devices.	Disclosure	s. 33.1(1)(b)

## 9. Risk Mitigation Table



# Privacy Impact Assessment for Zoom usage in MoH

PIA#: HLTH19050 / MoH#: 2019-11

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Employee and stakeholder personal information may be vulnerable on US stored Zoom server.	No use of Zoom cloud storage. User notification includes consent with use of Zoom that data and usage analytics will be collected by US based company Zoom.	Low	High
2.	Confidential information and or personal information including voice, visual and written communication may be leaked.	Recordings will only be saved to Government servers and not to Zoom cloud storage. Geolocation services will be disabled preventing additional disclosure potential. Collection notice will be included in each meeting invite.	Low	High
3.	Confidential documents may be leaked.	Documents will not be saved on the Zoom cloud storage only government servers.	Low	High
4.	Unauthorized collection, use or disclosure of recorded information from government server.	Recordings will be saved in a password protected LAN folder and only made available based on role and "need to know basis". Employees complete 1M 117 Information Management Course and adhere to PMAP and core privacy policy.	Medium	Medium
5.	Zoom is a foreign service subject to foreign laws	Changes to Zoom's Privacy Policy & Terms of Service will be tracked via updates through Zoom (links provided in security section). Implement best practice to limit amount of data stored on the Zoom server.	Very Low	High
6.	Inadvertently record individuals in background of meeting	Mitigate the risk of unintentional recording by using headsets and conducting meetings in private rooms.	Low	Med



# Privacy Impact Assessment for Zoom usage in MoH

PIA#: HLTH19050 / MoH#: 2019-11

		Those individuals who are inadvertently recorded will be notified and the recording deleted immediately.		
--	--	--	--	--

## 10. Collection Notice

*Personal information shared during this Zoom call may be collected by the Ministry of Health as per s. 26(c) of the Freedom of Information and Protection of Privacy Act and will be used to record minutes and conduct business activities. While no recordings will be saved to the Zoom storage cloud, Zoom conducts data and logs usage analytics including personal information such as IP address which may be shared with third parties and stored outside of Canada. By using Zoom you are consenting to the collection of your personal information by Zoom and its third-parties. Should you have any questions regarding the collection of this personal information please contact < organization > (telephone, email, physical address).*

## Part 3 – Security of Personal Information

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

*A paper copy of the Zoom password, account details and contact information of all those who have the account information, will be stored in a locked cabinet and access will only be made available to those involved with the project, program or activity that requires the use of Zoom.*

*The list will contain the names of staff members, date the account was created, employee signature agreeing to the STRA usage guidelines, date of signature and staff status (active/inactive).*

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

*Zoom is certified by SOC2, TRUSTe, and the EU-US Privacy Shield. Zoom has adopted security and privacy practices that make it compliant with Canada's Personal Information Protection and Electronic Documents Act as well as Ontario's Personal Health Information Protection Act.*

*Zoom utilizes a combination of industry-standard security technologies, procedures, and organizational measures to protect personal information. During the transfer of credit card information over the Internet, data is protected using Transport Layer Security (TLS) encryption technology.*

*Zoom cloud storage will not be used; any recordings made will be stored in a secure LAN folder on the government server after obtaining consent from individuals to record. Electronic copies of consent forms signed by participants will also be kept in a secure LAN folder. This folder will only be accessible to the account holder via IDIR verification. Passwords will be changed often and use a*



# Privacy Impact Assessment for *Zoom usage in MoH* PIA#: HLTH19050 / MoH#: 2019-11

---

*combination of upper and lower-case letters, numbers, and symbols and Zoom users will ensure that they use a secure browser.*

*A checklist document will need to be completed by program areas to determine whether an additional project PIA needs to be completed (Appendix A). The checklist will also provide guidance on how to safely use Zoom for ministry projects and activities. Finally, geolocation will be disabled during the use of Zoom by the Ministry.*

*A STRA has been completed on Zoom and reports no significant security issues. Please see STRA S2019-20 for additional security information.*

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

*The branch also adheres to the Privacy Management and Accountability Policy, the Ministry of Health Information Privacy Policy, and Ministry of Health Information Security Procedures.*

*Zoom's privacy policies may be accessed here <https://zoom.us/privacy>.*

*Zoom's security policies may be accessed here <https://zoom.us/security>.*

## **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.**

*Employees will have role-based access for account information and individual accounts will be password protected. Only a limited number of employees will have the passwords for the Zoom Account and key to the paper copy. Passwords will be changed in the instance of employee turnover.*

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

*The paper copy of the account information will be used as a tracking sheet.*

## **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?**

*Account information may be corrected by account holders. Recorded information may be deleted if necessary.*

*Meeting minutes may be annotated to indicate correction to any recorded information.*



# Privacy Impact Assessment for Zoom usage in MoH

PIA#: HLTH19050 / MoH#: 2019-11

---

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

*The collection of personal information will be limited in nature, voluntary and consented to for communication and document sharing purposes. Should Zoom be employed for collecting personal information and basing care or eligibility for services on the information collected, a separate PIA will be completed.*

**18. If you answered “yes” to question 16, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

*For the scope of the overarching PIA, individual users will have the ability to change their account information should there be any changes to their contact information. Recorded audio containing personal information that is no longer accurate may be deleted and documents may be corrected or annotated.*

**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?**

*For the scope of the overarching PIA, no personal information will be used to make decisions about individuals.*

## **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. However, if Zoom is employed in a program where identifiable information will be used for research or statistical purposes, a separate PIA will be completed.*

***Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact a PCT advisor.***

☐

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

*No.*



# Privacy Impact Assessment for *Zoom usage in MoH* PIA#: HLTH19050 / MoH#: 2019-11

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.*

\_\_\_\_\_  
Tim Perry  
Privacy Analyst  
Privacy, Compliance and Training  
Branch  
Corporate Information and  
Records Management Office  
Ministry of Citizens' Services

\_\_\_\_\_  
Signature

\_\_\_\_\_  
2020-03-18  
Date

\_\_\_\_\_  
Dwayne McCowan  
Manager, Privacy Operations  
Privacy, Compliance and Training  
Branch  
Corporate Information and  
Records Management Office  
Ministry of Citizens' Services

\_\_\_\_\_  
Signature

\_\_\_\_\_  
March 19, 2020  
Date

## **Part 7 – Program Area Comments and Signatures**



# Privacy Impact Assessment for *Zoom usage in MoH* PIA#: HLTH19050 / MoH#: 2019-11

---

Jeff Aitken signed in place of Eddy Piasentin		March 25, 2020
Don Stewart	Signature	Date
Gwen Lock	Gwen Lock Senior Manager, IMIT Security, HIPSL	March 26, 2020
Gwen Lock	Signature	Date
Corrie Barclay		May 19, 2020
Corrie Barclay Assistant Deputy Minister	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: Checklist and Conformation Page for Ministry of Health Zoom**



# Privacy Impact Assessment for

## *Zoom usage in MoH*

**PIA#: HLTH19050 / MoH#: 2019-11**

<b>Tool Use</b>	
<b>Go-Live Date</b>	
<b>Tool Administrator</b>	
<b>Phone</b>	
<b>email</b>	
<b>Branch</b>	
<b>Division</b>	

Please enter an X under the appropriate answer to the following questions:

	yes	no	N/A
<b>Purpose</b> Are you (the program area) using Zoom to do either of the following? <ul style="list-style-type: none"> <li>Conducting teleconference meetings for project management purposes; OR</li> <li>Sharing business documents for project management purposes</li> </ul> Please provide a description of the original purpose for employing the use of Zoom, including a description of the communication that will take place via Zoom (audio/video/document sharing). If Zoom will be used for the purposes of conducting interviews, consultations or appointments that require the collection of personal information such as for providing direct patient care, please skip this checklist and complete a privacy impact assessment.			
<b>Description:</b> <<<Please add description>>>			
<b>Collection Notification</b> The following Collection Notification (please see Appendix B) has been included in all meeting requests by email or a link to the meeting invitation on the webpage. The Collection Notification will include notification that there is the possibility of temporary storage outside of Canada. Please describe where the notification will be:			
<b>Description:</b> <<<Please add description>>>			
Participants using Zoom are providing only their own contact information and not information about another individual Participants will not use Facebook or Google to create login account, only business email address			
The amount of information stored on Zoom will be limited to non-personal information			
<b>Use</b> The information collected will be used only for the original purpose for which it was collected for			

For PCT Use Only:

Version 1.0



# Privacy Impact Assessment for *Zoom usage in MoH* PIA#: HLTH19050 / MoH#: 2019-11

Geolocation services will be disable on Zoom			
Voices and video of employees/contractors and stakeholders will only be streamed over Zoom and only saved to Government servers not on Zoom cloud storage			
<b>Disclosure</b> Zoom information is restricted to those that need to operate the account and those who are involved in the program/project/initiative/activity for which Zoom is being employed			
<b>Security</b> Saved Zoom recordings will be kept on a password protected LAN and accessed by those who need to know the information			
Meetings will be conducted in private meeting rooms or employ the use of headsets			
<b>Records Management</b> An approved records retention and deposition schedule is being used (please provide the ARCS and ORCS where available)			

**If you have answered “No” to any of the above questions separate PIA will need to be completed before you can use Zoom.**

Checklist Completed by:
Signature:
Program Manager Signature:
Date:
PCT Signature:
Date:

**PCT Comments:**

## **Appendix B – Checklist Collection Notification**



# Privacy Impact Assessment for

## Zoom usage in MoH

**PIA#: HLTH19050 / MoH#: 2019-11**

---

*Personal information shared during this Zoom call may be collected by the Ministry of Health as per s. 26(c) of the Freedom of Information and Protection of Privacy Act and will be used to record minutes and conduct business activities. While no recordings will be saved to the Zoom storage cloud, Zoom conducts data and logs usage analytics including personal information such as IP address which may be shared with third parties and stored outside of Canada. By using Zoom you are consenting to the collection of your personal information by Zoom and its third-parties. Should you have any questions regarding the collection of this personal information please contact < organization > (telephone, email, physical address).*



# 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:	<b>Paul Payne, Patient Empowerment Portfolio Lead, DHSI</b>		
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.



# Privacy Impact Assessment for MHSU VC PIA

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

---

- 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 operation. 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



# Privacy Impact Assessment for MHSU VC PIA

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

---

## 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](mailto:pia.intake@gov.bc.ca). A privacy advisor will be assigned to your file and will guide you through the completion of your PIA.



# Privacy Impact Assessment for MHSU VC PIA

PIA#: HLTH20103 / MoH#: 2020-57

---

## **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 Shiftwell 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:**

ExpressRoute 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 Application Gateway service (a load balancer and web application firewall).

#### **Azure Management Keys:**

As an additional access control option detailed in the Corporate PIA, Key Vault will be included with HDP's use of Azure to strengthen the transparency of access to data including Bring-Your-OwnKey capability and with the appropriate configuration enabling the activity and notification of logs every time the key is used (i.e. an event occurs).



# Privacy Impact Assessment for MHSU VC PIA

PIA#: HLTH20103 / MoH#: 2020-57

## 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.	<input type="checkbox"/>

## 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.	<input type="checkbox"/>



# Privacy Impact Assessment for MHSU VC PIA

PIA#: HLTH20103 / MoH#: 2020-57

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

Personal Information Flow Table			
	Description/Purpose	Type	FOIPPA Authority
1.	<p>BCEHS employees download, install and make use of the Shiftwell application, providing their information as requested.</p> <p>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).</p>	<p>Direct Collection (by PHSA)</p> <p>Indirect Collection (by Health)</p>	<p>s.26(c), (e) (PHSA)</p> <p>s. 27 (b) [33.1 (p)(i)]</p>
2.	<p>CGI and Freshworks provide technical support for Shiftwell 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.</p>	Use (by Health)	32(c) [33.1(p)(i)]
3.	<p>CGI and Freshworks provide production operational support for the Shiftwell 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).</p>	Use (by Health)	32(c) [33.1(p)(i)]



# Privacy Impact Assessment for MHSU VC PIA

PIA#: HLTH20103 / MoH#: 2020-57

## 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 developers 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 Key Management Service (KMS), Azure admins will not have access to them. Only designated MoH administrators and developers in the operations 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 ShiftWell 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 ShiftWell app account. After they have accepted and agreed to the Terms of Use and Privacy Policy a Verification Code is sent to the BCEHS employee using their @bcehs.ca email. The Verification Code 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.



# Privacy Impact Assessment for MHSU VC PIA

PIA#: HLTH20103 / MoH#: 2020-57

---

## **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 CGI/MoH/FW 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 provide Tier 2 and 3 support. Only Tier 3 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 Key Management System:

- 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
- Developers in the production operations groups will have access to manage the keys
- Production operations will be limited to a subset of developers who require elevated permissions strictly for production management. All activities and actions will be logged for audit compliance.



# Privacy Impact Assessment for MHSU VC PIA

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

---

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

1. Access request to PHSA for trusted CGI/Freshworks employee to access Azure
2. Approval from PHSA granted, now employee can access the production environment
3. Support Request comes through requiring data access. Approval must be provided by PO (Privacy Officer) and Freshworks 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 developers who must access the information for operational purposes.

While encryption keys are stored in Azure's Key Management Service (KMS), Azure admins will not have access to them. Only designated MoH administrators and developers 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:

GET\_REQUEST, POST\_REQUEST, PATCH\_REQUEST, DELETE\_REQUEST, ENTITY\_CREATED, ENTITY\_UPDATED, ENTITY\_REMOVED, USER\_LOGIN, INVALID\_SESSION\_LEVEL, INVALID\_USER\_TYPE, EMAIL\_NOT\_VERIFIED, INVALID\_SESSION, NOT\_PERMITTED, VERIFY\_ACCOUNT, CHANGE\_PASSWORD, USER\_LOCKED\_OUT, USER\_UNLOCKED, USER\_LOGOUT, SESSION\_UPGRADED, QUICKBLOX\_SESSION\_UPGRADED



# Privacy Impact Assessment for MHSU VC PIA

PIA#: HLTH20103 / MoH#: 2020-57

---

## **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



# Privacy Impact Assessment for MHSU VC PIA

PIA#: HLTH20103 / MoH#: 2020-57

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  
Privacy Analyst  
Privacy, Compliance and Training  
Branch  
Ministry of Citizens' Services

Signature

2020-10-14

Date

Dwayne McCowan  
Manager, Privacy Operations  
Privacy, Compliance and Training  
Branch  
Corporate Information and  
Records Management Office  
Ministry of Citizens' Services

Signature

2020-10-16

Date



# Privacy Impact Assessment for MHSU VC PIA

PIA#: HLTH20103 / MoH#: 2020-57

## Part 7 – Program Area Comments and Signatures

Paul Payne

Program Manager

Signature

November 4, 2020

[Click here to enter a date.](#)

Date

Ministry Contact Responsible for  
Security (Signature not required  
unless MISO has been involved.)

Signature

[Click here to enter a date.](#)

Date

Assistant Deputy Minister or  
Designate (if Personal Information  
is involved in this initiative)

Signature

[Click here to enter a date.](#)  
November 9, 2020

Date

Zen Tharani

Executive Director or equivalent (if  
no Personal Information is involved  
in this initiative)

Signature

[Click here to enter a date.](#)  
Nov 6, 2020

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 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:	<b>778 974-2705</b>
Program Manager:	<b>Leah Smith</b>		
Email:	Leah.Smith@gov.bc.ca	Phone:	<b>778 698-1340</b>

### **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.<sup>1</sup> 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*

<sup>1</sup> 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.



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

---

*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.*



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

---

*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).*

### **Overview**

*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*



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

---

- *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.*



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

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



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

<i>System Reporting (e.g. DAD)</i>	<i>Patient</i>	<i>Personal Health Number</i> <i>Date of Birth</i> <i>Gender</i> <i>Client Health Authority</i> <i>Admission date</i> <i>Discharge date</i> <i>HaH-specific codes that indicate that it is specifically a HaH occurrence</i>
<i>Clinical Monitoring Devices</i> <i>Remote Patient Monitoring</i>		<i>Patient biometric data including weight, blood pressure, pulse, glucose, pedometer, oxygen saturation, heart rate</i> <i>Standardized Clinical Assessment Tools and Surveys, including:</i> <i>General Anxiety Disorder (GAD -7)</i> <i>Patient Health Questionnaire (PHQ-9)</i> <i>Pain Disability Index (PDI)</i> <i>Virtual device information</i>
<i>Virtual Care</i>	<i>Patient</i> <i>Healthcare provider</i>	<i>Image and likeness, voice</i> <i>Virtual device information</i>
<i>On-Site Visits</i>	<i>Patient &amp; Caregiver</i>	<i>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,</i>



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

		<p><i>lifestyle information, procedural history, reason for visit, violence alerts and infectious disease precautions. Medical specialist diagnosis (e.g. mental health and substance abuse information).</i></p> <p><i>Please see appended schedules for a more comprehensive list of potential data collected.</i></p>
	<i>Healthcare provider</i>	<p><i>Healthcare provider name</i></p> <p><i>Practice/Specialty - Physician Specialty (Dermatology, Haematology &amp; Oncology, General Internal Medicine, Emergency Medicine, Gastroenterology, Immunology, Trauma, Intensivist).</i></p> <p><i>Along with professional opinion, medical record notes may include personal opinion.</i></p>
<i>Reports</i>	<i>Patient</i>  <i>Healthcare provider</i>	<p><i>Records shared with professional health care team such as GP or specialists may include any of the above listed data elements.</i></p> <p><i>Health authority reports shared with MoH may include the following data:</i></p> <ul style="list-style-type: none"> <li><i>• Date of referral</i></li> <li><i>• Medical Record Number</i></li> <li><i>• Referring physician</i></li> <li><i>• Acceptance or decline to HaH</i></li> <li><i>• Reason for decline</i></li> <li><i>• Patient deemed ineligible</i></li> </ul>



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

		<ul style="list-style-type: none"> <li>• Patient repatriation into hospital</li> <li>• Length of stay</li> </ul> <p>Health authorities may also keep incident logs detailing issues with workflows, patient or staff safety and similar details.</p> <p>Health authorities are to provide reports to the Ministry of Health including numbers on how many patients are accessing HaH.</p>
<i>Patient Safety &amp; Learning System</i>	<i>Patient</i> <i>Healthcare provider</i> <i>Caregiver</i>	<i>BCPSLS source of incidents reported which includes adverse event, negative outcomes, near miss, hazards.</i>
<i>Evaluation</i>	<i>Patient</i> <i>Healthcare provider</i> <i>Caregiver</i>	<p><i>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.</i></p> <p><i>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.</i></p> <p><i>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.</i></p>



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

<i>Transport</i>	<i>BC Ambulance Service</i> <i>Medivan</i> <i>Taxi</i>	<i>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.</i>
------------------	--	--

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.*



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

### 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
<b>If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.</b>	



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

### 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
<b>Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.</b>	

### 8. Personal Information Flow Table

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



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

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.	<p>HA Disclosure</p> <p>Public Transport Collection &amp; Indirect Use</p> <p>Private Transport Collection &amp; Indirect Use</p>	<p>s. 33.2(a)</p> <p>s. 27(1)(a)(i), (a.1)</p> <p>s. 26(c)</p> <p>s. 32(a)</p> <p>PIPA</p> <p>s. 8(1)</p> <p>s. 12(1)(a), (b)</p> <p>s. 14</p> <p>s. 15(a), (b)</p>
4.	<p>Health authority collects patient and healthcare provider personal information to manage and evaluate the HaH program.</p> <p>Research is considered out of the scope of this PIA.</p>	Collection Use	<p>s. 26(e)</p> <p>s. 32(a)</p>
5.	<p>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).</p> <p>Health authority also discloses adverse event data to MoH for reporting and investigation</p>	Disclosure	s. 33.2(a)
6.	MoH collects adverse event data from health authority involved.	Collection	s. 26(c), (e)



# Privacy Impact Assessment for Non-Ministry Public Bodies

## Hospital at Home – HLTH21003

	<p>MoH uses adverse event data to assess program safety.</p> <p>MoH shares adverse event data and program outcomes with health authorities across the province to improve program delivery and inform best practices.</p>	<p>Use</p> <p>Disclosure</p>	<p>s. 27(1)(b) [as per 33.2(a)]</p> <p>s. 32(a)</p> <p>s. 33.2(a), 33.2(l)</p>
7.	<p>Health authorities disclose patient financial information to MoH. This disclosure may include other third parties such as WCB, ICBC or private insurers.</p> <p>MoH collects patient financial information for the purposes of administering and managing MSP.</p>	<p>Disclosure</p> <p>Collection</p> <p>Use</p> <p>Disclosure</p>	<p>s. 33.2(a)</p> <p>26(c) [s. 5(e) of the Medicare Protection Act]</p> <p>32(a)</p> <p>33.2(a) [s. 49(2)(a) of the Medicare Protection Act and s.4(e) of the E-Health Act]</p>
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	<p>Health Authority contractual terms, privacy and security training.</p> <p>Auditing programs depending on health authority, please see</p>	Low	High



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

		<i>attached PIAs for more information.</i>		
2.	<i>Patient information may be compromised when healthcare provider is travelling between locations</i>	<i>Healthcare provider will employ reasonable security including device encryption, secure storage and supervision of documents. Please see security section for additional information.</i>  <i>Specific policies and processes developed by health authorities will be employed for the secure management of patient information while in transit.</i>	<i>Low</i>	<i>High</i>
3.	<i>Patient personal information may be compromised during virtual visits</i>	<i>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.</i>  <i>Please see appended schedules for security details.</i>	<i>Medium</i>	<i>High</i>
4.	<i>Patient information may be compromised in the Health Authority's information system</i>	<i>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.</i>	<i>Low</i>	<i>High</i>
5.	<i>The healthcare provider may unintentionally collect the personal information of non-HaH patients (family, friends etc.)</i>	<i>The healthcare provider will ensure there is privacy in the residence prior to treating patient.</i>  <i>Should it be necessary to collect non-patient personal information for the purposes of delivering care</i>	<i>Medium</i>	<i>Medium</i>



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

		<i>or documenting care that was provided, the healthcare provider will request permission and remove any identifying information where possible.</i>		
6.	<i>Patient may collect information about the healthcare providers when receiving care in their home</i>	<p><i>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.</i></p> <p><i>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.</i></p>	Low	High
7.	<i>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.</i>	<i>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.</i>	Medium	Medium
8.	<i>Adverse event reports may identify individuals and include sensitive personal information</i>	<i>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</i>	Low	High



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

		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.*



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

*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**



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

---

- 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.*



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

### **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.



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

---

### **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 Impact Assessment for Non-Ministry Public Bodies



## *Hospital at Home – HLTH21003*

### 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



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Hospital at Home – HLTH21003*

### **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



# **Privacy Impact Assessment for Non-Ministry Public Bodies**

## *Hospital at Home – HLTH21003*

---

### **Appendix A – Vancouver Island Health Authority PIA**



# 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<sup>1</sup>). 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,

---

<sup>1</sup> 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.



# Privacy Impact Assessment for Virtual Physician Pathways

PIA#: HLTH20051 / MoH#: 2020-32

---

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.



# Privacy Impact Assessment for Virtual Physician Pathways

PIA#: HLTH20051 / MoH#: 2020-32

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.

Data (including backups) at rest and in-transit is encrypted. Encryption keys are stored in Azure Key Vault – Bring Your Own Key (Key Vault). Key Vault enables users to store and use data through the protection of encryption keys. The Province would generate their own key onsite and then transfer it to Azure. One copy of the key is "put" in the cloud and the other copy is



# Privacy Impact Assessment for Virtual Physician Pathways

PIA#: HLTH20051 / MoH#: 2020-32

held by the Province. It will be inserted into a hardware security module (HSM) build on technology that the key cannot be extracted from. To mitigate the risk that the HSM is in Microsoft's possession, the Province has the ability to setup logs that can be viewed at any time related to the keys. Through these logs, the Province, either directly or through Bright Health, is able to view any use of the key (including if Microsoft uses the key without Province knowledge or consent).

## 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.	



# Privacy Impact Assessment for Virtual Physician Pathways

PIA#: HLTH20051 / MoH#: 2020-32

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

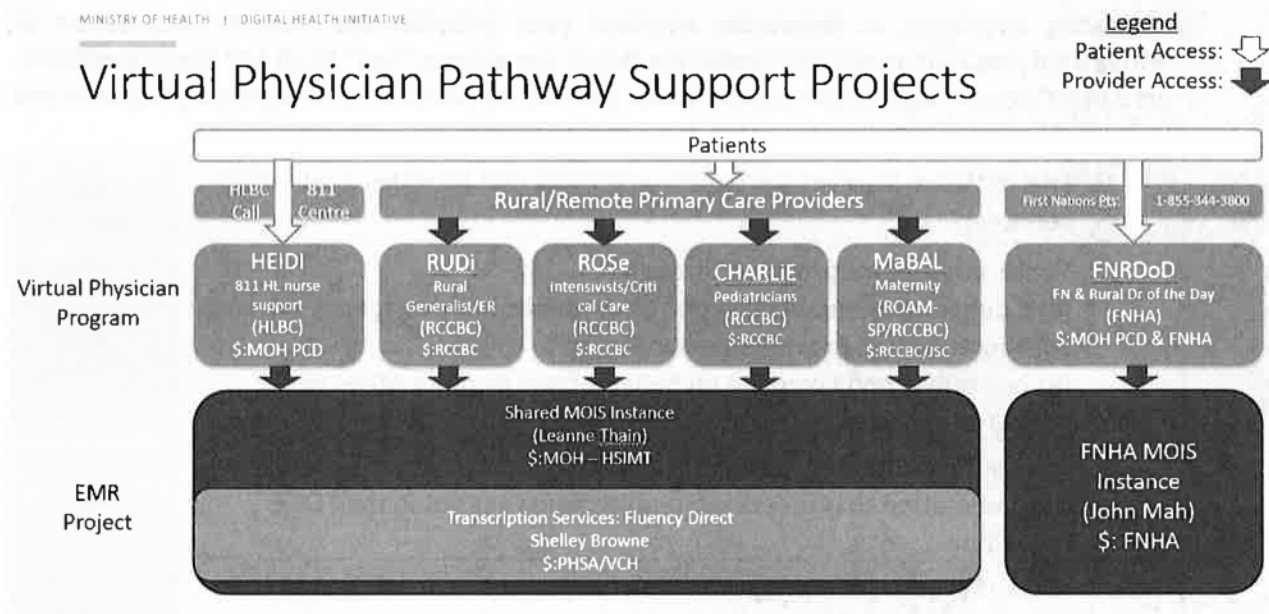
In FOIPPA, “common or integrated program or activity” is strictly defined. Answer the following questions to determine whether your initiative qualifies as “a common or integrated program or activity” under the Act. If you answer “yes” to all 3 of these questions, you must comply with requirements under 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
<b>Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.</b>	

# Privacy Impact Assessment for Virtual Physician Pathways

PIA#: HLTH20051 / MoH#: 2020-32

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



**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)



# Privacy Impact Assessment for Virtual Physician Pathways

PIA#: HLTH20051 / MoH#: 2020-32

	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**

	<b>Description/Purpose – Rural/Remote (R/R) Primary Care Providers</b>	<b>Type</b>	<b>FOIPPA Authority</b>	<b>Other Authority</b>
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)

For PCT Use Only:  
Version 1.0



# Privacy Impact Assessment for Virtual Physician Pathways

PIA#: HLTH20051 / MoH#: 2020-32

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 vGP's 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

# Privacy Impact Assessment for Virtual Physician Pathways

PIA#: HLTH20051 / MoH#: 2020-32

	storage, access and security of personal information as well as proper flow-through of requirements from government to service provider.	<p>vendor for inclusion within the contract. Vendor will be required to adhere to these schedules as per the agreement.</p> <p>In addition, these risks are mitigated through the use of Azure Key Vault (Bring-Your-Own Keys), which allows the Province to provide their own encryption keys, alongside visibility in the form of activity logs, which allows the Province to view any use of its keys without prior knowledge or consent.</p>		
4.	There is a risk of unauthorized access to personal information outside of Canada	<p>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). <i>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 mainly by the use of VM's as described above.</i></p> <p>The data is stored in Canada. Access to data at the infrastructure level is protected through the use of encryptions keys (Azure Key Vault) and visibility into activity logs will notify the Province in the event of unauthorized access.</p>		



# Privacy Impact Assessment for Virtual Physician Pathways

PIA#: HLTH20051 / MoH#: 2020-32

---

## 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 (HLBC KDR and ORCS LAN) 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: Username/password with Multi Factor Authentication. 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



# Privacy Impact Assessment for Virtual Physician Pathways

PIA#: HLTH20051 / MoH#: 2020-32

---

firewall. Login to MOIS uses 2-factor authentication (MFA - multi-factor authentication). All customer instances are managed in separate processes and accessed through different ports. Two layers of encryption are used: storage level full-disk encryption (AES 256 bit) and operating system level encryption. Backups are implemented via Azure Backup services which ensures encrypted backups. There are local and off-site backups. There is a disaster recovery site.

HEiDi - PDF versions of the Detailed Encounter Report are temporarily stored in an HLBC ORCS LAN folder until they are uploaded to the MOIS Cloud at which time they are then removed from the ORCS LAN folder.

MOIS MFA App (iOS or Android): Open OTP

MOIS server-side components:

- Various Azure infrastructure components including firewalls, Active Directory and storage
- RCDevs OpenOTP authentication server
- Various instances of Windows Server 2016 and 2019 hosting Windows Remote Desktop Services components
- Proprietary MOIS software
- Ubuntu hosting PostgreSQL

The MOIS Cloud sessions in the shared EMR instance are currently disconnected after 60 minutes of inactivity and all Personal Health Information (PHI) is cleared from the screen. Once sessions are disconnected, re-authentication, including MFA, is required to reconnect. Note that MOIS can be configured to lock the application and clear all PHI from the screen after any desired timeout. There is also a (currently non-configurable) backstop RDS idle timeout of 2 hours.

MOIS Cloud Accounts are locked out for 30 minutes after 6 failed logon attempts.

## **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



# Privacy Impact Assessment for Virtual Physician Pathways

PIA#: HLTH20051 / MoH#: 2020-32

---

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 Tier 1 technical support.

Bright Health has OS-level and database admin level accounts which are needed to maintain the system and individual accounts are assigned to each person. All logons are logged. Only a few Bright Health employees have admin access and only on a need basis. All access requires MFA.

Bright Health currently provisions and revokes access to the HealthLink instance of MOIS based on instructions from HealthLink. Bright Health provisions an Administrator account to a designated HealthLink user for which the password should be changed after the customer-designated Administrator first logs on. The Administrator then creates groups, roles and assigns privileges.

MOIS has comprehensive, highly configurable application audit trails. Whatever auditing you'd like to do is achievable. By default, MOIS maintains a comprehensive audit trail (create, read, update and delete) on user access to data in patients' charts.

#### Limiting Microsoft Access:

All components of MOIS in Azure that have access to PHI are in VMs 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 top of the VMs. Microsoft personnel have no access, administrative or otherwise, to these VMs: they have no accounts, logins or user logins. As such, the technical barriers to access by Microsoft personnel are exceptionally high and would require significant circumvention of their normal security policies, procedures and systems. E.g. they would have to hack into the machines to obtain access and even if they disabled the hardware encryption, there would still be a layer of software encryption.

#### **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 credentials (username and password) which can be tracked (Bright Health can review access if desired).



# Privacy Impact Assessment for Virtual Physician Pathways

PIA#: HLTH20051 / MoH#: 2020-32

---

## **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



# Privacy Impact Assessment for Virtual Physician Pathways

PIA#: HLTH20051 / MoH#: 2020-32

## **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

Privacy Analyst

Privacy, Compliance and Training  
Branch

Corporate Information and  
Records Management Office  
Ministry of Citizens' Services

Signature

16 October 2020

Date

Dwayne McCowan

Manager, Privacy Operations

Privacy, Compliance and Training  
Branch

Corporate Information and  
Records Management Office  
Ministry of Citizens' Services

Signature

October 23, 2020

Date



# Privacy Impact Assessment for Virtual Physician Pathways

PIA#: HLTH20051 / MoH#: 2020-32

## Part 7 – Program Area Comments and Signatures

Leanne Thain

Program Manager (HSIMIT)

Signature

January 13, 2021

Date

Sandra Sundhu

Program Manager (HLBC)

Signature

October 29, 2020

Date

Gwen Lock

Ministry Contact Responsible for  
Security (Signature not required  
unless MISO has been involved.)

Signature

2021-01-13

Date

Corrie Barclay

Assistant Deputy Minister or  
Designate (HSIMIT)

Signature

January 13, 2021

Date

Ted Patterson

Assistant Deputy Minister or  
Designate (HLBC)

Signature

October 29, 2020

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

---

## Appendix A – vMOA scripts

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

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.



# Privacy Impact Assessment for Virtual Physician Pathways

PIA#: HLTH20051 / MoH#: 2020-32

---

**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 Ministries (MPO Format)

### PART 1: GENERAL INFORMATION

**Initiative Title**

Foundry Virtual Care Application 2020-98

**PCT Intake Number**

HLTH21005

**Name of Ministry**

Ministry of Health

**Name of Branch or Unit**

Health Sector IM/IT

**PIA Drafter (Your Name)**

Wynne MacAlpine

**Your Work Phone**

236-478-1191

**Your Email**

wynne.macalpine@gov.bc.ca

**Initiative Lead Name** (this will appear in the [Personal Information Directory](#))

Kimberly Moulton

**Initiative Lead Phone** (this will appear in the [Personal Information Directory](#))

250.952.3174

**Initiative Lead Email**

Kimberly.Moulton@gov.bc.ca

**Ministry Privacy Officer**

Sukhy Sidhu

**Ministry Privacy Officer Phone**
**Ministry Privacy Officer Email**

HealthInformationPrivacy@gov.bc.ca

**FOR MINISTRY PRIVACY OFFICER (MPO) USE ONLY**

**1. Type of PIA:**

PI-PIA

**2. Is this a data-linking initiative under FOIPPA?**

No

**3. Related PIAs:**

CITZ20038 – Microsoft Azure Cloud Services (Corporate PIA)

HLTH20017-HDPI Phase 2 (Health PIA 2020-04)

HLTH20103 (Health PIA 2020-57)

**4. Is this a common or integrated program or activity?**

No

**5. I do not agree to share this PIA for this reason:**

N/A

**6. Would you describe this as a high risk or complex initiative?**

No

If yes, describe what makes this initiative high-risk or complex.

**7. Provide a brief summary of the initiative to be published in the Personal Information Directory. This summary may be similar to the answer to question 1 below.**

The Foundry Virtual Applications Project is a project by the Ministry of Health, Ministry of Mental Health and Addictions and Foundry BC, under Providence Health Care, to develop a virtual care platform comprising mobile and web applications. The virtual care platform will directly connect patients to Foundry services without the need to visit a physical support location. The Ministry of Health (MoH) will be providing back-end technical and development support to enable the operation of the platform and ongoing Tier 2 and 3 Help Desk Support to Foundry service providers and clients. CGI and Freshworks have

been contracted by the MoH to that end. This PIA covers the Ministry of Health's technical and development support for the virtual care platform through CGI and Freshworks.

## 1 Describe your initiative

Describe your initiative in enough detail that a Privacy Advisor who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.

The Mental Health and Substance Use (MHSU) Virtual Clinic Limited Production Roll-Out Project has undertaken two initiatives to create and pilot virtual clinic platforms for online access to therapy and support tools for individuals with mild to moderate mental health or substance use challenges: the BC Emergency Health Services Commission (EHS) Shiftwell Application and The Foundry Virtual Applications Project. The EHS Shiftwell Application is reviewed in PIA HLTH 20103 (MoH 2020-57). This PIA reviews the Foundry Virtual Mobile and Web Applications Project.

The Foundry Virtual Applications Project is a project by the Ministry of Health, Ministry of Mental Health and Addictions and Foundry BC, under Providence Health Care, to develop a virtual care platform comprising mobile and web applications. The virtual care platform will directly connect patients to Foundry services without the need to visit a physical support location.

The virtual care platform will:

- Provide integrated, clinically supervised, online mental health and substance use peer support, primary care, and social services and supports through a single technological solution.
- Increase the availability and geographic accessibility of confidential early intervention services by complementing and augmenting existing services.
- Support continuity of care using technology to support secure information sharing.
- Provide a storage space for dependable and recommended health resources to diminish the risks associated with search engine commercial optimization.
- Develop innovative and acceptable technology solutions that enable and empower individuals to access support online and take an active role in their care.

The Ministry of Health is the intellectual property owner for the platform. The Ministry's role is to:

- own platform licenses and handle license distribution;
- provide IT support and maintenance (for bugs & enhancements that require an IT Vendor);
- fund the STRA for the platform;
- manage the technical deployment of the platform; and
- provide ongoing Tier 2 and 3 Help Desk Support on the platform to Foundry service providers and clients.

FreshWorks and CGI are vendors subcontracted by the Ministry to complete the development work on the mobile and web applications, provide licensing, IT support and maintenance, technical deployment and ongoing Tier 2 and 3 Help Desk Support.

Foundry will act as the business owner for the platform. Its role is to:

- Provide ongoing operational support;
- Manage platform development for release in early 2021.
- Provide Tier 1 Help Desk Support on the platform to Foundry service providers.
- Implement platform in Foundry BC.
- Provide ongoing evaluation of platform benefits.

Foundry will own all privacy and security functions for the project and is responsible for the development and completion of a PIA on Foundry's use of the virtual care platform. Foundry BC is responsible for the development and completion the Terms of Use and Privacy Policy required for the Applications. While the Ministry has procured a third-party vendor to perform Penetration Tests and develop the STRA, identifying any risks and remediations, Foundry is responsible for acknowledging and addressing findings according to remediation plans, and understanding the risks associated with unmitigated vulnerabilities.

## 2 Describe the scope of your PIA

Your initiative might be part of a larger one or might be rolled out in phases. What part or phase of the initiative is covered by this PIA? What is outside of the scope of this PIA?

The Ministry of Health (MoH) will be providing back-end technical and development support to enable the operation of the platform and ongoing Tier 2 and 3 Help Desk Support to Foundry service providers and clients. CGI and Freshworks have been contracted by the MoH to that end. This PIA covers the Ministry of Health's technical and development support for the virtual care platform through CGI and Freshworks. The use of the platform itself is not being assessed in this PIA, which has been addressed by Foundry, Providence Health Care PIA 2018-0144.

## 3 Describe your information or data

Please list all the elements of personal information or data that you might collect, use, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information.

The virtual care platform will collect the following personal information directly from patients/clients (young persons):

- full name, preferred name, pronoun and gender;
- date of birth;
- email address, phone number, postal code;
- personal health number;
- emergency contact;
- written story – a free text field where young person can share what they want a service provider to know about them.
- health survey responses – intake surveys to help connect young person with services they need;
- client self-assessments - standard assessment tools completed by young person;
- satisfaction/feedback surveys - for quality and service improvement.
- demographics survey - for service improvement purposes and to inform care.

The virtual platform will also collect information from young persons in collaboration with service providers:

- Clinical (Diagnostic, Treatment & Care) Action Plans - allows young person to keep track of their goals, activities and tasks they want to achieve.
- Medication – allows young person to keep track of the medications they are taking.

Other information collected by the virtual platform includes:

- Clinical and case management notes - entered by service provider to document care or service in the EMR.
- Service use data (i.e. purpose of visit) - To understand services being used (evaluation) and so a care provider and young person has access to their journey. Automatic collection based on service accessed.

Ministry contractors may have access to this personal information in its back-end technical support and Helpdesk role.

## Check a box

Did you list personal information in question 3? Personal information is any recorded information about an identifiable individual other than business contact information. Personal information includes information that can be used to identify an individual through association or inference.

**Yes**, my initiative involves personal information.

Check the box and get in touch with your [Ministry Privacy Officer](#) (MPO) and fill out [parts 2](#) to 6 of the template with your MPO's help (skip question 4).



**No**, my initiative does not involve personal information

Check the box and complete question 4 below. Submit questions 1 to 4 to your Ministry Privacy Officer (MPO). You do not have to complete the rest of the PIA template.



## 4 Risk assessment for projects with no personal information

Some initiatives that do not require personal information contain a high risk of collecting personal information inadvertently, which could result in a privacy breach. Use this section to identify how you reduce the risk of unintentionally collecting personal information.

n/a

## PART 2: PROTECTION OF PERSONAL INFORMATION

Part 2 asks you to think through how you will protect personal information that you collect, use, store, access or disclose.

### Check a box

If your project involves a cloud-based solution.

If **yes and you have consent** to store or access personal information outside Canada

Check the box and continue to question 6.



If **yes and you do not have consent** to store or access personal information outside Canada

Check the box and contact your Ministry Privacy Officer (MPO) to discuss the cloud solution you're using.

Your MPO will provide a list of questions to answer about privacy and cloud. Skip question 5 and go to question 6.



If **no**

Check the box and go to question 5.



## 5 Storing personal information

In most cases FOIPPA requires that personal information is stored and accessed only in Canada. FOIPPA requirements are designed to reduce the likelihood that British Columbians' personal information is subject to the laws of another country.

If your initiative meets one of three conditions, you may be authorized under FOIPPA to store or access personal information outside Canada.

### 5.1 Is all personal information stored and accessed in Canada?

Yes.

Client 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 the application platform within Canada. All storage and access of personal information (including backups) occurs within the secure networks/servers of the PHSA, which are located within Microsoft Azure's Canadian region only.

5.2 If you answered 'No,' refer to FOIPPA section 30.1 and indicate which condition might allow you to store or access personal information outside of Canada.

Select

## 6 Collection, use and disclosure

This section will help make sure you have the authority to collect, use and disclose personal information and that you limit your collection where possible.

Your MPO will help you identify whether each step represents collection, use or disclosure and make sure you have legal authority for what you want to do. Your MPO completes the blue section of this table.

Additional rows can be added. If your program is complex you may want to create a diagram or flow chart and attach it to this PIA.

MPO use only

Describe the way <u>personal information</u> moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	use, collection, disclosure	FOIPPA Authority	Other legal authority
<p>Foundry clients download, install and make use of the mobile and web application, providing their information as requested.</p> <p>The information is stored in servers managed by TELUS (under contract by PHSA). The Ministry of Health (MoH) 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).</p>	<p>Direct Collection (by Foundry)</p> <p>Indirect Collection (by MoH)</p>	<p>s.26(c), (e) (Foundry)</p> <p>s. 27 (b) [33.1(1)(p)(i)]</p>	
CGI and Freshworks provide levels 2 and 3 technical support for platform 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 staff need to conduct significant technical maintenance and repairs.	Use (by MoH )	32(c) [33.1(1)(p)(i)]	
CGI and Freshworks provide production operational support for the platform. In the course of their work, they will have the ability to view and access PI stored in the platform. This access will only occur when staff need to make significant changes to the application or for extraordinary requests (e.g. subpoena).	Use (by MoH)	32(c) [33.1(1)(p)(i)]	

Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how all the different parts are connected. This is optional.

## 7 Collection notice

FOIPPA states that a public body needs to provide a written or verbal collection notice when it collects

personal information directly from the individual it is about.

Write your collection notice. FOIPPA requires that you include:

- The purpose for your collection
- The legal authority in FOIPPA for collecting it
- The title, business address and business phone number of an employee who can answer questions about the collection

An email address is optional.

A collection notice is not needed as the PHC/Foundry BC has their own collection notice and the Ministry is collecting information indirectly under s.27 (b) for the purpose of the virtual care platform.

### FOR MINISTRY PRIVACY OFFICER USE ONLY

Check the box if a collection notice is not required as per section 27 (3) or (4) of FOIPPA. ☒

## PART 3: SECURITY OF PERSONAL INFORMATION

In part 3 you will share information about the privacy aspect of securing personal information. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical (e.g. your office building) and technical (e.g. the online cloud service) environments. What security measures are in place?

### Check a box

If your initiative involves a digital tool, database or information system.

#### If yes

You need to involve your MPO and possibly your Ministry Information Security Officer (MISO). Together you can decide whether your initiative needs a Security threat and risk assessment (STRA).

Check the box if you have or will have a completed STRA. ☒

If you already have the STRA number, enter it here: enter STRA number here

Skip part 3 and go to part 4.

#### If no

Check the box and complete part 3. ☐

## 8 Physical security

8.1 Are all physical records stored in government buildings with government security?

No

8.2 If you answered 'No,' describe the physical security you have in place to protect the records.

There are no physical records. All records are digitized and follow the technical security measurement as described in section 9 Technical security.

8.3 Describe any additional physical security measures specific to this initiative.

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.

## 9 Technical security

9.1 Are all records stored on government servers?

Yes

9.2 If you answered 'No,' describe the technical security you have in place to protect the records

Only MoH, CGI/FW 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 provide Tier 2 and 3 support. Only Tier 3 support will have potential access to the Applications data. They would not be evaluating or changing data information and do not have any intention of sharing the information with Foundry/PHC 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 Key Management System:

- 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
- Developers in the production operations groups will have access to manage the keys
- Production operations will be limited to a subset of developers 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 PHSA for trusted CGI/Freshworks employee to access Azure
2. Approval from PHSA granted, now employee can access the production environment
3. Support Request comes through requiring data access. Approval must be provided by PO (Privacy Officer) and Freshworks manager

9.3 Describe any additional technical security measures unique to your program area.

#### **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 the virtual care platform within Canada.

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

#### **Routing**

ExpressRoute 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 Application Gateway service (a load balancer and web application firewall).

#### **Azure Management Keys**

As an additional access control option detailed in the Corporate PIA, Key Vault will be included with the Health Data Platform's use of Azure to strengthen the transparency of access to data including Bring-Your-Own Key capability and with the appropriate configuration enabling the activity and notification of logs every time the key is used (i.e. an event occurs).

## 10 Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

1 We only allow employees in certain roles to access information

☐

2 We require a digital key to access digital records

☒

3 Employees that need standing or recurring access to personal information must be approved by executive lead

☐

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

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

4 We use audit logs to see who accesses a file and when

☒

5 Additional controls

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

Encryption keys are stored in Azure's Key Management Service (KMS), but Azure admins will not have access to them. Only designated MoH administrators and developers in the operations group will have access to the keys.

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:

GET\_REQUEST, POST\_REQUEST, PATCH\_REQUEST, DELETE\_REQUEST, ENTITY\_CREATED, ENTITY\_UPDATED, ENTITY\_REMOVED, USER\_LOGIN, INVALID\_SESSION\_LEVEL, INVALID\_USER\_TYPE, EMAIL\_NOT\_VERIFIED, INVALID\_SESSION, NOT\_PERMITTED, VERIFY\_ACCOUNT, CHANGE\_PASSWORD, USER\_LOCKED\_OUT, USER\_UNLOCKED, USER\_LOGOUT, SESSION\_UPGRADED, QUICKBLOX\_SESSION\_UPGRADED

## PART 4: ACCURACY, CORRECTION & RETENTION

In part 4 you will demonstrate that you make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

### 11 Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a plan in place to respond to these requests.

11.1 Do you have a process in place to correct personal information?

Yes

The Ministry of Health Master Service Agreement (MSA) with CGI requires CGI and its subcontractors to ensure compliance with FOIPPA and the Province's FOIPPA Policy and Procedures Manual.

11.2 Sometimes it's not possible to correct the personal information. Will you make a note on the record that the correction was requested, if you're not able to correct the record itself?

Yes

CGI's and FreshWorks' work may include updating and correcting personal information belonging to Foundry clients through technical support. However, Foundry clients and service providers are expected to update and correct their own personal information.

11.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party of the request. Will you ensure that you conduct these notifications when necessary?

Yes

CGI and FreshWorks follow the processes and requirements as described in the FOIPPA and the Province's FOIPPA Policy and Procedures Manual.

### Check a box

Does your initiative use personal information to make decisions that directly affect an individual? For example, you might use an individual's date of birth or income information to determine their entitlement to a benefit, or you might use employment history in a job competition.

If yes

Check the box and answer question 12.

☐

If **no**

Check the box, skip question 12 and continue to part 5.

☒

## 12 Decision affecting individuals

Provide information about how you use personal information to make decisions that directly affect an individual.

12.1 Describe what decisions are made that directly affect individuals and what personal information is used to make the decisions.

12.2 How will you make sure that the personal information is accurate and complete?

12.3 FOIPPA requires that Ministries keep personal information for a minimum of one year after it was used to make a decision. Do you have an approved information schedule in place related to this information?

yes/no

12.4 If you answered 'No,' describe how you will ensure this information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

## PART 5: AGREEMENTS AND INFORMATION BANKS

Please provide a bit more information about whether your initiative will involve a research agreement, information sharing agreement or personal information bank.

### Check a box

Does your initiative include or be part of a regular and systematic exchange of personal information with

partners in or outside government? If so, you may require an information sharing agreement (ISA).

If **yes**

Check box and continue with question 13.

☐

If **no**

Check the box, skip question 13 and continue to the next yellow box.

☒

## 13 Information Sharing Agreement (ISA)

Below, list the organizations involved in the information sharing agreement and explain what personal information you regularly exchange.

Description of ISA:

Name of main ministry or agency involved:

List other ministries, agencies, public bodies or organizations involved:

Business contact title for person responsible for maintaining the ISA:

Business contact phone number for person responsible for maintaining the ISA:

ISA start date:

Select start date

ISA end date:

Select end date

### Check a box

Does your initiative involve sharing personal information with a third party for research or statistical purposes?

If **yes**

Check box and continue with question 14

☐

If **no**

Check the box, skip question 14 and continue with the next yellow box

☒

## 14 Research Agreement

Please list the third parties with whom you disclose personal information and the purpose for which personal information will be used in the research. Attach your completed research agreement to this PIA.

### Check a box

Will your initiative result in a personal information bank? A personal information bank (PIB) is a collection of personal information searchable by name or other unique identifier.

If **yes**

Check box and continue with [question 15](#)

☐

If **no**

Check the box and go to [question 16](#)

☒

## 15 Personal Information Bank (PIB)

Please describe your personal information bank in the table below.

Description:

Name of main ministry or agency involved:

List other ministries, agencies, public bodies or organizations involved:

Business contact title:

Business contact phone number:

## PART 6: ADDITIONAL RISKS

Part 6 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

## 16 Risk Response

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template.

**1. Risk:**

Employees could access personal information and use or disclose it for personal purposes.

**Response:**

Only certain CGI/Freshworks staff will have permissions that enable them to view personal information, and for strictly production management purposes. Their activities are audited and logged.

PHC/Foundry BC staff are not granted any purposeful access to information stored within Azure.

**2. Risk:**

Someone other than authorized staff accesses encryption keys.

**Response:**

While encryption keys are stored in Management Service (KMS), Azure admins will not have access to them. Only designated MoH administrators and developers in the operations group will have access to the keys.

**3. Risk:**

Information provided by user in the app does not belong to its actual owner

**Response:**

Foundry BC clients/service providers will download the 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 an app account after they have accepted and agreed to the Terms of Use and Privacy Policy. There is a one-time, 6-digit, system generated, random, anonymous verification code used when a user registers. This code is sent to the user's email as entered during registration to verify their email identification.

## PART 7: SIGNATURES

PCT will create a summary of the review.

## PCT Summary

PCT recognizes that the MoH's role in this project is to provide back-end technical and development support to enable the operation of the platform and ongoing Tier 2 and 3 Help Desk Support to Foundry service providers and clients.

### Risk Rating

Low Risk



No Risk	Low Risk	Medium Risk	High Risk	Critical Risk
No risks are associated with this initiative...	Risk exists and is tolerable....	Risk should be reduced but may be tolerated...	Risk should be reduced but may be tolerated for a short period...	Unacceptable risk which cannot be justified except in very special circumstances...

### Risk Treatment Plan

- PCT did not recommend an OIPC consultation
- While the collection, use, and disclosure of personal information required to complete this MoH role is seen to be authorized under FOIPPA by PCT, PCT is not reviewing the Foundry's operation of the program, nor it's related FOIPPA 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 Manager or Director Only required if personal information is involved
Cole Lance, Privacy Advisor	Quinn Fletcher, Director
	
2021-01-26	2021-01-26

## Ministry Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their MPO and if necessary, complete a PIA update to submit to PCT. Your ministry may choose to add signatories.

### Comments

Add comments here

Initiative Lead	Name of Executive Director  *Not required if ADM signs	Name of Assistant Deputy Minister or designate  *Only required if personal information is involved
Paul Payne	Enter name of Executive Director	Corrie Barclay
	Enter signature of Executive or Director	Enter signature of ADM
2021-01-29	Date signed by Executive Director	Date signed by ADM

Ministry Privacy Officer	Name of person responsible for information security  *Only required in case a Ministry Information Security Officer (MISO) has been involved
Enter name of MPO	Enter name of MISO
Enter signature of MPO	Enter signature of MISO
Date signed by MPO	Date signed by MISO



# 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](mailto: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.*



# Privacy Impact Assessment for *MHSU Virtual Clinic* PIA#: HLTH18048 / MoH#: 2018-36

---

*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:*



# Privacy Impact Assessment for *MHSU Virtual Clinic* PIA#: HLTH18048 / MoH#: 2018-36

---

- 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



# Privacy Impact Assessment for *MHSU Virtual Clinic* PIA#: HLTH18048 / MoH#: 2018-36

---

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.

<sup>1</sup> 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.



# Privacy Impact Assessment for *MHSU Virtual Clinic* PIA#: HLTH18048 / MoH#: 2018-36

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](mailto: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

Privacy Analyst  
Privacy, Compliance and Training  
Branch  
Ministry of Citizens' Services

Signature

21 November 2018

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

Click here to enter a  
date.

Date



# Privacy Impact Assessment for *MHSU Virtual Clinic* PIA#: HLTH18048 / MoH#: 2018-36

## Part 7 – Program Area Comments and Signatures

Jane London  
Project Director

Signature

*Jane London*

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.***