Privacy and security in virtual health

RESOURCE FOR PHSA CLINICIANS

- The Office of Virtual Health works closely with PHSA's privacy and security leaders when considering how best to select, implement and use various virtual health solutions.
- There are some unique risks when using technology to provide care virtually.
  - *The Notification for the Use of Digital Communications form is a resource that can be shared with patients.*
- PHSA and other health organizations are mandated by law to protect personal information through BC's Freedom of Information Protection of Privacy Act (FIPPA), including in the context of virtual health.
  - *Learn more about privacy and PHSA on this POD page.*

This resource is meant to support PHSA staff and clinicians in navigating privacy and security in virtual health.

KEY DEFINITIONS

VIRTUAL HEALTH

Virtual health is a care model focused on connecting citizens, families and clinicians, using technology to optimize wellness, enhance care, and improve outcomes.

VIRTUAL PRIVATE NETWORK (VPN)

VPN is a service that creates a safe, encrypted, online connection when using a public network.

PRIVACY

In a virtual health context, privacy is how a health organization collects, uses, discloses, stores and secures personal information in accordance with BC privacy laws.

ENCRYPTION

Encryption scrambles your information so that it is inaccessible to unauthorized users—making it difficult to steal your passwords, credit card numbers and other personal information. PHSA virtual health visits are encrypted.

SECURITY

Security is the act of protecting computer systems, networks and data from cyber attacks. This is done through safeguards including security awareness education, policies, industry best practices, procedures and software controls.

*An example of **security** is using a secure system like Zoom for Healthcare to communicate with patients about their health instead of a clinician's personal email. On the other hand, **privacy** policies limit patient health record access to only a patient's care team, and also set guidelines around who can use a clinical virtual health tool.*

Created by Office of Virtual Health – Education. **Effective date: Jan 7, 2022**

Provincial Health Services Authority
Province-wide solutions. Better health.

Office of Virtual Health
Connecting for health

FAQ'S FROM CLINICIANS

Q: Do I need to remind patients at each visit of the potential security risks?

A: Not at every visit, but **definitely at the first** and then repeated as needed. Patients need to be made aware of the potential risks as part of the informed consent process. Any questions from patients about security risks, at any point during their virtual care, should be appropriately addressed. For more information on consent in relation to virtual health, please refer to the PHSA Virtual Health Handbook.

Q: What are my responsibilities to help prevent a privacy breach during my virtual health visit?

A: PHSA privacy recommends the following:

- Review this POD page on privacy breaches
- Review the appropriate education/resources/training for each virtual health tool
- Read the Terms of Use for each virtual health tool
- Make sure you're on VPN (Virtual Private Network) or your health authority (HA) network
- Make sure you're signed in with your HA account
- Know who you're expecting in a virtual health appointment and confirm identity before you begin
- Avoid making any consultation notes on paper. If you do – they must be secured (ie: locked cabinet)
- Do everything on your HA issued laptop/mobile device if possible

Q: What should I do in the event of a privacy breach?

A: Immediately inform your manager and follow the direction as per the Managing Privacy and Confidentiality Breaches Policy.

Q: What do I need to know about patient privacy and security training for virtual health?

A: There is general required training on privacy and security for all PHSA staff. There is no specific privacy and security training for virtual health. However, information specific to virtual health privacy and security information can be found on this POD page, and on the IMITS security page. Information about Zoom privacy and security can be found in this online course, the full manual, and the terms of use.

Q: Where can I find more information?

A: IMITS Security Awareness Hub – resources by the IMITS Information Security team on how to protect yourself and your patients.

Office of Virtual Health (OVH) webpage – learn about OVH and find resources on specific virtual health tools (e.g. Zoom for Healthcare), such as this Zoom security best practices resource.

Virtual Health Handbook – information and references that consider professional standards, current legislation and feedback from PHSA subject matter experts. Intended to support PHSA staff using virtual health in their clinical practice.

MORE QUESTIONS?

Email us at: officeofvirtualhealth@phsa.ca

Provincial Health Services Authority
Province-wide solutions. Better health.

Office of Virtual Health
Connecting for health

POSSIBLE QUESTIONS FROM YOUR PATIENTS

Q: Do I need to be in a private space for my virtual health appointment?

A: Yes**.** As personal health information may be discussed, having a private space is important. **This is no different from when care is given in person**. However, others are welcome to come to your appointment as needed, and with your permission (e.g., family, friends, translator etc.).

Q: Should I be worried about privacy breaches in my virtual health appointment? How do I know this interaction isn't being intercepted?

A: Just like any online service where you are asked to give personal information (e.g. online banking), privacy breaches are possible. PHSA highly values the privacy and security of our patients and their personal information. We are ordered by BC's privacy law, and also keep our own privacy, security, and clinical professional standards to make sure that our patients are protected.

We work closely with experts to only choose virtual health tools that meet a specific security standard, and we also provide guidelines on how to safely and securely use these tools. There are also things you can do to help protect your privacy such as using antivirus software, using a secure Wi-Fi network, protecting your passwords and only downloading software from trusted sources.

Q: Why can't I use public Wi-Fi?

A: Public Wi-Fi is not always safe to use because you don't know who set it up, or who else is connecting to it (e.g. hackers). Therefore, we recommend that you use a secure Wi-Fi, like your personal home Wi-Fi or a VPN. See this IMITS Security page for more information.

Q: How do I know you are not recording this session?

A: We would ask for your permission before any recording. If recording were to happen using Zoom, you would see a red circle on your screen and hear a sound notification that recording is in progress.

Q: What are you going to do with my information after my virtual health visit?

A: Your personal health information is entered into your health record. For electronic health records (EMR), there are safeguards in place protecting access, as well as policies and laws for appropriate use.

Q: Who has access to my information?

A: Just as we would during an in-person visit, PHSA staff and health care clinicians collect personal information to confirm your identity, and make notes about the visit within your health record. Only those clinicians involved in your care can view your personal health information.

Q: Where is my information kept, and how long is it stored for?

A: Information is kept within your electronic health record or within your paper chart in a clinic. The Records Retention/Disposal Data Health Records Policy has schedules showing the amount of time clinical records must be stored.

DID YOU KNOW?

For tech support, your patients can call: Patient Virtual Health Care Tech Support at 1-844-442-4433 (toll-free)

Provincial Health Services Authority
Province-wide solutions. Better health.

Office of Virtual Health
Connecting for health