FEBRUARY 2021

Privacy and security considerations for virtual health care visits

GUIDELINES FOR THE HEALTH SECTOR

The delivery of virtual health care has become an integral part of Ontario's health system. Virtual health care can include secure messaging, telephone consultation, and videoconferencing. These forms of digital communication offer significant convenience for health information custodians (custodians) and their patients where physical distance poses a challenge. However, virtual health care also raises unique privacy and security concerns because it depends on technologies, communication infrastructures, and remote environments. Virtual health care raises new kinds of cybersecurity risks that are not as prevalent in the analog world.

PHIPA applies to virtual care as it does to in-person care.

Ontario's health privacy law, the *Personal Health Information Protection Act* (*PHIPA*), applies to virtual care as it does to in-person care. Custodians must comply with the provisions of *PHIPA*, in addition to all other applicable laws and regulations, as well as guidance issued by relevant professional regulators.

In this guide, we recall some of the key requirements in *PHIPA* relevant to all custodians, including those who operate in a virtual health care context. We then provide some practical steps custodians should take to protect personal health information, particularly as they plan and deliver virtual health care.

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

KEY *PHIPA* REQUIREMENTS

The following key *PHIPA* requirements apply to all custodians, whether they provide in-person or virtual health care:

Data minimization

- Custodians must not collect, use, or disclose personal health information if other information serves the purpose of the collection, use, or disclosure.
- Custodians must not collect, use, or disclose more personal health information than is reasonably necessary to meet the purpose of the collection, use, or disclosure.

Safeguarding

- Custodians must take steps that are reasonable in the circumstances to ensure that personal health information is protected against theft, loss, and unauthorized use or disclosure and that records are protected against unauthorized copying, modification, and disposal.
- Custodians must ensure that records are retained, transferred, and disposed of securely.

Custodians must ensure that records are retained, transferred, and disposed of securely.

Electronic service providers

If a custodian uses an electronic service provider, both the custodian and the provider are subject to additional obligations. These other obligations depend on whether the electronic service provider is an *agent* of the custodian.

If the provider is an *agent* of the custodian, they are acting with the custodian's authorization, for or on behalf of the custodian, and not for their own purposes.

In the case of an *agent*, the custodian:

- remains responsible for any personal health information that is collected, used, disclosed, retained, or disposed of by the agent
- must take reasonable steps to ensure that the agent does not collect, use, disclose, retain, or dispose of personal health information unless it:
  1. is permitted by the custodian
  2. is necessary for carrying out their duties as an agent
  3. is not contrary to *PHIPA* or any other law
  4. complies with any conditions or restrictions imposed by the custodian

If the provider is an agent of the custodian, they are acting with the custodian's authorization, for or on behalf of the custodian, and not for their own purposes.

For their part, the electronic service provider, as an *agent* for the custodian, must:

- comply with the four conditions above
- notify the custodian at the first reasonable opportunity in the event of a privacy breach

If the service provider is ***not*** an agent of the custodian, then other limitations apply. Unless otherwise required by law, the electronic service provider must ***not***:

- use any personal health information to which they have access in providing services for the custodian, except as necessary to provide the services
- disclose personal health information to which they have access in providing services for the custodian, or
- permit their employees, or any person acting on their behalf, to have access to the information, unless the employee or person agrees to comply with the restrictions that apply to the electronic service provider.

Health information network providers

The provision of health care often involves communications between multiple custodians. A health information network provider is a type of electronic service provider who delivers electronic services to two or more custodians primarily to enable communication with one another. Health information network providers are subject to additional obligations under *PHIPA*, including to:

Health information network providers are subject to additional obligations under *PHIPA*.

- keep an electronic log of all accesses to and transfers of personal health information and make it available to the custodians on request
- notify custodians of any incidents of unauthorized access
- provide a plain language description of their services and safeguards to the custodians
- publicly post this description, along with any relevant directives, guidelines, and policies
- perform privacy impact assessments and threat risk assessments and provide copies of the results to the custodians
- ensure that any third party they retain to assist in providing services to the custodians abides by the same restrictions and conditions to which they are themselves subject
- have a written agreement with the custodians describing the services offered and the safeguards in place to ensure the confidentiality and security of personal health information, and requiring the network provider to comply with *PHIPA*

STEPS TO ENHANCE PRIVACY AND SECURITY IN VIRTUAL HEALTH CARE

Laying the groundwork

Custodians should start by determining which statutory rules and professional or other regulatory guidelines apply to them and ensure they understand these obligations. Custodians should check with any applicable regulated health colleges and be aware of their policies and any other applicable laws, besides *PHIPA*, that may require additional duties with respect to virtual health care.

Custodians should also develop and implement a virtual health care policy.

Custodians should conduct **privacy impact assessments** to identify and manage the specific privacy and information security risks associated with providing virtual health care. To learn more, see the IPC's ***Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act***.

Custodians should also develop and implement a **virtual health care policy**. The policy should address the specifics of when, how, and the purposes for which health care may be provided virtually, any conditions or restrictions in doing so, and what administrative, technical, and physical safeguards will be in place. The policy should explicitly state that employees and other agents will have access to only the minimum amount of personal health information necessary to perform their duties. Custodians should notify their patients about their virtual health care policy.

Comprehensive privacy and security training is essential for reducing the risk of unauthorized collection, use, and disclosure of personal health information. Custodians should ensure their employees and other agents participate in ongoing privacy and security training, including training on their organization's virtual health care policies and the specific circumstances that arise in the virtual health care context. If the custodian's employees and other agents work remotely, they should be given specific direction and guidance to mitigate the associated privacy and security risks. For more information, see the IPC's fact sheet, ***Working from Home During the COVID-19 Pandemic.***[1]

Custodians must have a robust **information security management framework** to regularly monitor, assess, and mitigate any security risks that may arise in the course of using the virtual platform. The framework must include all of the required administrative, technical, and physical safeguards expected of employees, other agents, and any electronic service providers. These include ongoing obligations to implement and update access controls, maintain audit logs, regularly monitor for and

1 This Fact Sheet applies to public sector and government organizations; however, many of the recommendations and best practices set out in it apply to custodians as well. If there is any conflict between what is set out in this Fact Sheet and the requirements of *PHIPA*, custodians must comply with *PHIPA*.

apply software updates, and conduct regular audits and threat risk assessments.

The IPC expects custodians to have a **privacy breach management protocol** in place that sets out the requirements related to the identification, reporting, containment, notification, investigation, and remediation of actual and suspected privacy breaches. The obligation to report privacy breaches at the first reasonable opportunity to affected individuals, and in certain situations to the IPC, continues to apply in a virtual context. To learn more about what to do when there is a privacy breach, see the IPC's ***Responding to a Health Privacy Breach: Guidelines for the Health Sector*** and ***Reporting a Privacy Breach to the IPC: Guidelines for the Health Sector***.

The IPC expects custodians to have a privacy breach management protocol in place.

Selecting the vendor

To assist custodians in choosing virtual visit solutions, Ontario Health has developed a **Virtual Visits Solution Standard.** This provincial standard was developed to help custodians and vendors deliver secure virtual health care by using "safe, secure and interoperable platforms".[2] The standard sets out the mandatory requirements that must be satisfied for a product or service to be designated as a verified solution by Ontario Health. As solutions are verified, a list of them will be published **online** to help guide custodians in making their selection.

Custodians should consider how the solutions they are considering procuring for virtual health care integrate with their overall information management infrastructure. They must ensure the solutions they use comply with applicable interoperability specifications established by Ontario Health.

Custodians who engage third-party service providers in the delivery of virtual care should ensure, through contractual agreements, that the service providers comply with the privacy and security measures to satisfy the requirements set out in *PHIPA*. Among other contractual undertakings, the service provider should agree to:

- immediately notify the custodian in the event of a privacy breach
- undergo periodic security audits at the request of the custodian
- restrict access to personal health information by employees or any person acting on their behalf on a need-to-know basis
- securely return or destroy information at the end of the agreement

Custodians should not engage the services of providers that require, as a condition of service, that individuals register with the service provider or accept terms of service and privacy policies that require collection, use, or disclosure of personal information or personal health information for purposes unrelated to the custodians' provision of care.

2 Custodians remain responsible for ensuring that they continue to comply with the requirements of *PHIPA* when using a virtual care solution provided by a vendor who has participated in Ontario Health's Virtual Visits Solution Standard verification process.

Preparing for virtual visits

Before booking a virtual visit, custodians should determine if a virtual visit is even appropriate, considering their patient's needs, computer and technical requirements, the purpose of the visit, and relevant regulatory guidance.

Custodians should also consider both the risks and benefits of holding the visit virtually rather than in person. This includes practical mobility and accessibility factors for their patients, as well as their own ability to uphold their obligation to protect the privacy and security of the patient's personal health information in a virtual setting.

Custodians should also consider both the risks and benefits of holding the visit virtually rather than in person.

Obtaining patient consent

Using plain language, custodians should inform their patients of the limitations and risks of virtual care visits, including potential privacy breaches resulting from physical or electronic eavesdropping, hacking and software exploits, technical failures, and configuration errors.

Custodians must have the patient's consent to collect, use, and disclose personal health information through virtual care technologies and services. Custodians should document the discussion of the limitations and risks of virtual care visits, including the potential for privacy breaches, and the consent obtained. The patient should be informed that they can withdraw this consent at any time.

Putting in place effective safeguards

Custodians must put in place technical, physical, and administrative safeguards to protect personal health information. Proper planning is crucial for ensuring virtual visits are as private and secure as possible.

Custodians should avoid using personal email, unencrypted text messaging, or free cloud-based videoconferencing platforms to communicate with patients. These platforms raise serious privacy risks. Custodians should have safeguards in place to protect personal health information through secure email, messaging, or conferencing systems that have been vetted and approved for use by their organization. Some examples of safeguards include:

Use only organization-approved email, messaging, or videoconferencing accounts, software, and related equipment.

Technical safeguards:

- use only organization-approved email, messaging, or videoconferencing accounts, software, and related equipment
- use firewalls and protections against software threats
- regularly update applications with the latest security and anti-virus software

- encrypt data on all mobile and portable storage devices, both in transit and at rest[3]
- maintain, monitor, and review audit logs
- use and maintain strong passwords
- review and set default settings to the most privacy protective setting
- verify and authenticate a patient's identity before engaging in an email exchange, chat, or videoconference

Keep all technology containing personal health information, such as desktop computers and servers, in a secure location.

Physical safeguards:

- keep all technology containing personal health information, such as desktop computers and servers, in a secure location
- keep portable devices containing personal health information, such as smartphones, tablets, and laptops, in a secure location, such as a locked drawer or cabinet, when they are unattended
- restrict office access, use alarm systems, and lock rooms where equipment used to send, receive or store personal health information is kept
- do not lend technology containing personal health information to anyone without authorization
- ensure there are no unauthorized persons in attendance or within hearing or viewing distance
- physically segregate and restrict access to servers to only authorized persons

Ensure employees and other agents are properly trained to use secure email, messaging, and videoconferencing platforms.

Administrative safeguards:

- ensure employees and other agents are properly trained to use secure email, messaging, and videoconferencing platforms
- adopt a robust system of access controls and regularly maintain authorizations on a need-to-know basis
- ensure employees and other agents are well aware of their ongoing obligation to avoid collecting, using or disclosing more personal health information than is necessary
- ensure confidentiality agreements contain explicit provisions dealing with employees' and other agents' obligations when using secure email, messaging, or videoconferencing to deliver virtual health care

3 The IPC does not consider the loss or theft of an electronic device containing encrypted personal health information to be a privacy breach (a term that encompasses security breaches involving personal health information) where the risks of unauthorized access to unencrypted information are demonstrably low. However, whether or not the information is encrypted, custodians should require employees and their other agents to report any such loss or theft. This will enable custodians to determine, on a case-by-case basis, whether the information was properly protected.

Safeguarding against privacy and security risks in virtual care is an ongoing obligation. Custodians should continue to monitor for and address cybersecurity threats, for example by:

- updating software regularly
- providing ongoing security training to employees and other agents to support the detection of phishing attempts
- conducting regular threat risk assessments

Additional safeguards for email

The following discussion focuses on communicating personal health information by email. Similar rules should apply to communicating personal health information by secure messaging.

One of the unique challenges for custodians using email to communicate with their patients — *particularly when they cannot see or hear the patient* — is to ensure the exchange is with the correct person. Custodians should verify the recipient's identity and correctly address emails or messages to avoid misdirection. One approach is to send a test message in advance and ask for confirmation to ensure the message reaches the intended recipient.

Further safeguards to use when communicating personal health information by email include:

- providing a notice in an email that the information received is confidential
- providing instructions to follow if an email is received in error
- communicating by email from professional rather than personal accounts because personal accounts may have weaker security levels and may be more susceptible to compromise
- confirming an email address is up to date
- ensuring that the recipient's email address corresponds to the intended address
- regularly checking pre-programmed email addresses to ensure that they are still correct
- restricting access to the email system and to email content on a need-to-know basis
- informing patients of any email address changes
- acknowledging receipt of emails
- minimizing the disclosure of personal health information in subject lines and message contents to the greatest extent possible
- ensuring strong access controls to email accounts used by custodians
- recommending that patients use a password-protected email address that only they can access

Custodians should also ensure compliance with the safeguards specified in any other policies and procedures, including those related to using personal devices in the workplace.

Patients should be registered through a secure messaging solution that authenticates their identity before accessing their messages.

Custodians should use encryption for emails to and from patients that contain personal health information. This includes by encrypting or password-protecting document attachments and sharing passwords separately through a different channel or message. If the use of encryption is not feasible, custodians must determine if the use of unencrypted email is reasonable in the circumstances after considering all relevant factors, including the sensitivity of the information, the purpose of the transmission, and the urgency of the situation (please see IPC's ***Fact Sheet: Communicating Personal Health Information by Email***). Custodians are also expected to use encryption when emailing personal health information to other custodians.

Custodians should use encryption for emails to and from patients that contain personal health information.

Custodians' employees, other agents, and patients should be reminded of the risks associated with *phishing* to avoid falling prey to malware, spyware, or other forms of social engineering. Phishing is an online attack in which an attacker — using both technological and psychological tactics — sends a message designed to trick the recipient into revealing confidential information or downloading malware. Phishing attacks often imitate legitimate sources and work by exploiting people's trust, curiosity, fear, and desire to be helpful and efficient. Recipients should be cautious when faced with messages that are unexpected or contain suspicious attachments or links.

Custodians should store personal health information on email servers only for as long as is necessary to serve the intended purpose. For example, if email communication is documented in the patient's record, it may not be necessary to retain duplicate copies of the information on an email server. Likewise, custodians should ensure that all copies of emails containing personal health information on portable devices are securely deleted when they are no longer needed and are documented in the patient's record.

For best practices, please see the IPC's fact sheets ***Communicating Personal Health Information by Email*** and ***Protect against Phishing***.

Additional safeguards for videoconferencing

When using videoconferencing platforms to deliver care, custodians should take additional steps to prepare the patient for their virtual visit. For example, the custodian could ask about captioning or screen reader requirements to address accessibility concerns and review the steps the patient can take to protect their privacy.

As a best practice, both the custodian and the patient should join the videoconference from a private location using a secure internet connection. This includes using a closed, soundproof room or an

As a best practice, both the custodian and the patient should join the videoconference from a private location using a secure internet connection.

otherwise quiet and private place and having window coverings where and as appropriate. Use headphones rather than the speaker on the device to prevent being overheard by others, and be mindful of where screens are positioned.

Once logged into the videoconference, the custodian should check the meeting settings to ensure the meeting is secure from unauthorized participants. If the software or application can record the meeting, this feature should only be used when it is necessary and the patient provides express consent.

At the start of an initial visit, the custodian should verify the identity of the patient. In the event of a new patient encounter, the custodian should compare the patient's image with a photo on file or ask the patient to hold up their health card to the camera for confirmation.

The custodian should introduce themselves and any others who are present on the custodian side of the interaction and ensure the patient consents to the presence of any additional individuals. The custodian should also inquire if anyone is accompanying the patient and confirm the consent of the patient.

When videoconferencing, custodians must use sufficiently high-quality sound and resolution to ensure they are able to collect information (including verbal and non-verbal cues) that is as accurate and complete as is necessary for the purpose of providing health care.

Custodians may consider seeking feedback from patients to ensure they feel secure using digital platforms.

After the virtual visit

Custodians should document virtual interactions with patients in the same manner as in-person interactions as part of the patient's record. The same record retention requirements apply to virtual interactions, and patients continue to have the same access and correction rights.

Custodians may consider seeking feedback from patients to ensure they feel secure using digital platforms and that they are not reluctant to share information for fear of privacy and security risks.

About patient portals

Custodians may choose virtual care solutions that are part of their electronic medical record systems, such as patient portals. Depending on the functionality or type of platform, patients may be able to view their test results and records, manage their appointments, and exchange messages with the custodian via the portal.

Custodians should inform patients of the types of information available through the portal, to whom it is accessible, and how long that information will remain in the portal, in addition to any privacy and security implications.

Given the variety of patients' health literacy levels, custodians should consider how to assist patients in understanding the information displayed in the portal. If the portal allows patients to contribute

information, such as blood pressure readings, pain scales, or social and behavioral data, the patient should understand if and when the custodian will review the information.

The custodian must have the patient's consent to collect, use, and disclose personal health information through the portal. Custodians must also consider and set up appropriate access controls for substitute decision-makers when required. If the patient would like to delegate access to the portal to someone else or transfer or export some of the information for other purposes, such as sharing information with an employer or an insurance company, the custodian and patient should discuss the implications and the most privacy-protective way to enable this.

Custodians must ensure there are appropriate safeguards in place with respect to portal access. This includes developing a procedure for the patient's initial access, and the subsequent identification and authentication required when the patient's logs into the portal.

Custodians should provide clear guidance to patients on the secure and private configuration and use of the portal. This includes encouraging patients to use strong passwords and explaining the risks associated with sharing passwords or taking and sharing screen shots. Custodians should educate their patients about the importance of accessing the portal in a discreet and private setting and logging out of the portal after each session. As an important backup, custodians should configure the portal by enabling a default setting that automatically logs users out after a certain period of inactivity.

The custodian must have the patient's consent to collect, use, and disclose personal health information through the portal.

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario