Ontario Health

Virtual Visits Verification Privacy Guidance
PIA Summary Playbook

Date Last Reviewed & Published – June 2025

Ontario Health outlines the requirements that Virtual Care Solution Providers must demonstrate to be verified as compliant with Ontario Health's standard for virtual visits ("standard").[1] The purpose of the Virtual Visits Verification (VVV) Program is to support Solution Providers, health care organizations and clinicians to develop and use privacy and security enhanced solutions and services in accordance with applicable laws, regulations, and industry standards. Ontario's health privacy law, *Personal Health Information Protection Act, 2004* (*PHIPA*)[2], applies to virtual care as it does to in-person care. Health Service Providers (HSP) or Health Information Custodians (as referred to in *PHIPA)* must comply with all applicable laws and regulations, such as *PHIPA*, and any guidance issued by relevant regulators. Participation in the VVV Program is voluntary. Information about the program is found at https://ontariohealth.ca/verification.

Some key definitions available in Appendix C

Virtual visits involve the collection, use, disclosure, retention, and/or transmission of personal health information (PHI) and personal information (PI). In addition, access, transfer and disposal, when required, of PHI/PI are fundamental to the solution capabilities. Maintaining privacy while delivering care using virtual visit solutions involves unique challenges that can lead to unintended risks, such as data breaches. Solution Providers can mitigate many of these risks by implementing appropriate privacy and security policies, procedures, and practices including conducting of Privacy Impact Assessments (PIAs). Mitigation includes taking reasonable steps to confirm that technologies used by HSPs to provide health care to patients enable PHI/PI to be shared in a private and secure manner.

Privacy Impact Assessments (PIAs) are used to evaluate the potential privacy risks posed with the collection, use, disclosure of PHI/PI, and to implement mitigation strategies. They are an important part of safeguarding data and data breach preparedness and can evaluate whether your organization has incorporated sufficient data privacy protections and compliance to legislative and regulatory requirements. PIAs are an opportunity for organizations to identify privacy issues *before they become problems*. The submission of a **PIA Summary** is **THE** requirement of the VVV Program. **Ontario Health does NOT collect NOR require the full-length PIAs.**

In this Playbook, Ontario Health elaborates on some key privacy requirements from *PHIPA* and the VVV Program relevant to all HSPs and Solution Providers. Solution Providers can use these

[1] Virtual Visits Verification Standard
[2] Personal Health Information Protection Act, 2004

steps to assist them in completing their PIAs in accordance with requirements as specified in the standard.

Following is a list of the mandatory VVV Privacy Requirements that must be reflected in Solution Provider **PIA Summary** submissions. **PIA Summaries** should include, at a minimum:

- Date that Full-Length PIA was completed
- Date PIA Summary was completed

Solution Providers ***must*** meet all **mandatory** requirements. Solution Providers ***may*** meet **recommended** requirements but are not required to. Recommended requirements may in future become Mandatory.

Req. #	Requirement Description example
2.3.1: Publish a notice of its information practices relevant to its virtual visit solution and services.	The notice must describe how the Solution Provider manages PHI/PI, including a general description of safeguards in relation to that information. This description shall include the practices that apply to the virtual care services the Solution Provider provides to health care organizations, clinicians, and patients.
2.3.2: Have a designated employee responsible for privacy.	The name or title and contact information for the person who is accountable for the Solution Provider's privacy program including privacy policies and practices must be publicly and easily accessible on the Solution Provider's website. A generic email address (i.e. privacy@abc.com) is acceptable. The email must be directed to the employee responsible for privacy and/or the provider's Privacy Office.
2.3.3: Have a privacy and security program that includes policies and procedures.	Solution Provider must have a privacy policy that outlines rules governing the collection, use, disclosure, retention, accuracy, security and disposal of PHI/PI, breach management, information security, business continuity and disaster recovery, access, correction, and complaint practices.
2.3.4: Provide an electronic audit log of all virtual visit encounters including a log of all accesses and transfers of PHI	The electronic audit log must include: • the type of PHI viewed, handled, modified, or dealt with. • the date and time PHI was viewed, handled, modified, or dealt with. • the identity of all persons who viewed, handled, modified, or dealt with PHI. • the identity of the individual to whom PHI relates.
2.3.7 Provide an up-to-date PIA summary.	Statement that the PIA Summary reflects the full-length PIA.
	Statement that PIA findings have been approved by organization leadership including individual responsible for privacy.
	Name of individual who completed full-length PIA.

Req. #	Requirement Description example
	Person completing PIA Summary meets the following qualification requirements from the International Association of Privacy Professionals (IAPP): • CIPP/C • CIPM • CIPT **OR** Minimum of two years of experience conducting PIAs in health care setting in Ontario and/or Canada.
	Confirmation that PIA was conducted using the Information Privacy Commissioner of Ontario's template for health care[3] or similar. This could be reflected by including the Table of Contents from full-length PIA where it states what template was used.
	The full-length PIA must meet recency requirement of being conducted no longer than 2 years prior to the VVV submission date. Confirmation that full-length PIA reflects the latest solution design and technical architecture with no significant changes to the solution, services, or privacy program.
	The Solution Provider lists the role (s) that PHIPA identifies and why authority applies.[4]
	Summary includes table of contents from the full-length PIA and reflects that Fair Information Principles from Canadian Standards Association were used in privacy/legal analysis (Appendix B).
	Summary should include: • an overview of the solution/technology/service that has been assessed by the full-length PIA specifically the Secure Messaging and/or Video modality; • description of modality; • authentication procedures; • practice management/billing (electronic medical record); • appointment booking/reminders (email, secure messaging system); • business analytics/intelligence; • solution support.
	The summary reflects legislative analysis for PHIPA; FIPPA where applicable.

[3] PIA Guidelines for Health Care

[4] PHIPA applies to a wide variety of persons and organizations defined as health information custodians. PHIPA also applies to agents who are authorized to act for or on behalf of custodians. Additionally, PHIPA applies to the use and disclosure of personal health information by those who receive personal health information from custodians (recipients) and to electronic service providers, including health information network providers. PIA FAQ Sep 2015

Req. #	Requirement Description example
	Table containing identified risks stating whether a risk has been classified as high, medium, or low. Heat map is not acceptable (see below)
	Risk table contains clear mitigation recommendation(s) for each risk finding and provides a status on any outstanding risks as of the date of full-length PIA report. **(A sample risk table is available in Appendix A)** **NOTE:** Risks identified as **High** must be mitigated prior to VVV submission. Summaries will be returned to Solution Provider for resolution
	Risks identified as **Medium** must have a mitigation plan with timelines for closure within six months of date of full-length PIA Report. Ontario Health may ask for confirmation that risk mitigation has been completed.
	Low risks should be identified and have mitigation plan within 12 months from the date of the full-length report.
2.3.8: Meet security controls assurance requirements [5]	Reference that an information security assessment completed one of: 1. SOC 2 Type 2 Audit Report 2. ISO 27001 certification 3. HITRUST certification 4. OMD Certified EMR listed on OntarioMD's website **NOTE: Local Solution Providers can meet this requirement by submitting a TRA report and attesting to security operational controls.** The PIA Summary should reference completion of one of the above requirements.

[5] **PHIPA Security**
12 (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. 2004, c. 3, Sched. A, s. 12 (1).

Req. #	Requirement Description example
2.3.12: Provide a comprehensive agreement framework for the virtual visit solution and related services including for any third party retained to assist in providing the agreement framework	Solution Provider may engage and use data processors or third parties who will require access to PHI/PI. Provide a list of all third parties involved in delivery of solution (see table): • company name, • agreement(s) in place which describes the services and the administrative, technical and physical safeguards relating to the confidentiality and security of PHI and PI and how the Solution Provider and any third-party Solution Provider retained comply with applicable legislation, • nature and purpose of processing, • data elements shared with sub-processor, • location of data storage. **See table in Appendix A**
2.3.13: Support health care organizational or clinician retention obligations and policies	Confirmation of retention of PHI in accordance with record keeping and retention obligations and policies of HSPs (i.e. 10 years+)
2.3.14: Ensure all PHI data as defined in PHIPA is held by systems located in Canada.	Solution must be hosted within a Canadian location including all PHI, data, and backups.
2.3.15: Inform users including patients if any PHI data as defined in PHIPA flows outside of Canada	A confirmation that Access and transient PHI must only flow outside of Canadian borders with prior consent from the user.

Ontario Health

Appendix A: Sample tables for PIA Summary

1. Risk Table

Risk Scenario: (High level statements)	**Risk Rating:** (Low/Medium/ High)	**Recommendations:**	**Risk Treatment Status:** (Mitigated, Transferred, Avoided, Accepted, In Progress)

2. Third-Party Sub-Processor Chart

Sub-processor name. NOTE: Confirm that Agreement in Place.	**Nature and purpose of Processing**	**Data Elements shared with sub-processor**	**Location of sub-processor's data centre**

Ontario Health

Appendix B: CSA Model Code for the Protection of Personal Information Fair Information Principles or FIPs (CAN/CSA-Q830-96)

1. **Accountability**: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
2. **Identifying Purposes**: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. **Consent**: The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate.
4. **Limiting Collection**: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. **Limiting Use, Disclosure, and Retention**: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information shall be retained only as long as necessary for fulfilment of those purposes.
6. **Accuracy**: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
7. **Safeguards**: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. **Openness**: An organization shall make readily available to individuals' specific information about its policies and practices relating to the management of personal information.
9. **Individual Access**: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. **Challenging Compliance**: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

Ontario Health

Appendix C: Definitions of Key Concepts

Agent

- A person who is authorized by a custodian to perform services or activities in respect of PHI on the custodian's behalf and for the purposes of that custodian.
- May include a person or company that contracts with, is employed by or volunteers for a custodian and, as a result, may have access to PHI.
- *PHIPA* permits custodians to provide PHI to their agents only if the custodian is permitted to collect, use, disclose, retain or dispose of the information.

Source: Frequently Asked Questions: Personal Health Information Protection Act, Sept 2015 (IPC-O)

Control

- Over a record or PHI/PI.
- Being accountable for it, including ensuring the protection of privacy, and being able to make decisions about how it is to be managed.
- Regardless of who has been assigned custody of a record or PHI/PI, it is considered to be under an institution's control when the institution has the duty and authority to manage it, including restricting, regulating, and administering its use, disclosure, or disposition.

Custody

- Refers to having physical possession of a record or PHI/PI.
- Does not equate to control.
- Service provider may have custody of a record or PHI/PI, but it does not have control.
- In the context of an agreement with a service provider, control and responsibility for a record or PHI/PI collected on behalf of an institution must be retained by the institution, even though it is processed or stored by a service provider.

Electronic Service Provider (eSP)

- A person who supplies services that enable a custodian to collect, use, modify, disclose, retain or dispose of PHI electronically.
- If not an agent of the custodian, then it shall not use any PHI to which it has access in the course of providing services to the custodian, except as necessary in the course of providing the service and it cannot disclose the information.
- Must also ensure their employees or any other persons acting on their behalf agree to comply with these restrictions.

Source: Frequently Asked Questions: Personal Health Information Protection Act, Sept 2015 (IPC-O)

Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31 (FIPPA)

Ontario legislation with two main purposes: 1) to make provincial government institutions more open and accountable by providing the public with a right of access to records; and 2) to

protect the privacy of individuals with respect to their Personal Information held by provincial government organizations. References to FIPPA include the regulations made thereunder, as may be amended or replaced from time to time.

Health Information Custodian (HIC)
A person or organization listed in *PHIPA* that, as a result of power, duties or work set out in *PHIPA*, has custody or control of PHI.
Source: Frequently Asked Questions: Personal Health Information Protection Act, Sept 2015 (IPC-O)

Health Information Network Provider (HINP)
- A specific type of eSP.
- A person who provides services to two or more custodians, where the services are provided primarily to enable the custodians to use electronic means to disclose PHI to one another, whether the person is an agent of any of the custodians.

Source: Frequently Asked Questions: Personal Health Information Protection Act, Sept 2015 (IPC-O)

Health Service Providers (HSP)
May include solo practitioners, clinics, home and community care organizations, hospitals or any other HSP type that is fully or in part funded by the Ministry of Health.

Health Service Provider Innovator
Has developed a virtual care solution, independently or in partnership with other HSPs and/or Solution Providers.

Personal Health Information (PHIPA Section 4 (1))
- Means **identifying information** about an individual in oral or recorded form, if the information:
  (a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
  (b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual…..
  (d) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual…..
  (f) is the individual's health number.
- **Identifying information** means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual. (2004, c. 3, Sched. A, s. 4 (2))
- PHI includes identifying information that is not PHI (i.e. personal information)….but that is contained in a record that contains PHI (2009, c. 33, Sched. 18, s. 25 (3)).

Ontario Health

Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A (PHIPA).
The Ontario health privacy law. It establishes rules for the management of PHI and the protection of the confidentiality of that information, while facilitating the effective delivery of health care services. References to PHIPA include the regulation made thereunder, as may be amended or replaced from time to time.

Personal information (FIPPA Section 2 (1))

- Means recorded information about an identifiable individual, including,
    a. information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
    b. information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
    c. any identifying number, symbol or other particular assigned to the individual,
    d. the address, telephone number, fingerprints or blood type of the individual,
    e. the personal opinions or views of the individual except where they relate to another individual,
    f. correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
    g. the views or opinions of another individual about the individual, and
    h. the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.
- Does not include the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity. (2006, c. 34, Sched. C, s. 2.)

Privacy Impact Assessment (PIA) key aspects

- A "point-in-time" self-assessment, organizational risk management tool and process used to identify the effects of a given process or other activity on an individual's privacy.
- Serve to identify any risks to the institution.
- Review the impact that a proposed information system, technology or program may have on the privacy of an individual's personal health information under *PHIPA.*
- A valuable due diligence exercise, identifies and addresses potential privacy risks that may occur in the course of operating a proposed or existing information system, technology or program.

Source: Planning for Success: Privacy Impact Assessment Guide May 2015

- Should help you identify, analyze, and address key privacy risks when changing or developing programs or systems, including those involving service providers.
- Understanding privacy risks can help you take appropriate and timely action to ensure you comply with legislation and other requirements.

- Also can help make informed policy, business, procurement, architecture, and security decisions.

Source: IPC Guidance: Privacy and Access in Public Sector Contracting with Third Party Service Providers

- a formal risk management tool used to identify the actual or potential effects that a proposed or existing information system, technology or program may have on individuals' privacy.

Source: Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act October 2005

Processing

Includes the collecting, using, disclosing, retaining, storing, securing, or disposing of records or PHI/PI.

Solution Provider or Third-Party Solution Provider

Providers of virtual care solutions that are required to meet all Mandatory Requirements for patient-to-provider video and/or secure messaging, as applicable and as specified in these Virtual Visits Solution Requirements. May be solution vendors, Health Service Provider Innovators (HSP Innovators), or Local Solution Providers

Appendix D: Disclaimer

This document is intended to be used as a guide and not as a legal advice. The guide is intended to aid organizations in determining their obligations under PHIPA, FIPPA and other applicable legislations. While this guide is a helpful reference, it is not a substitute for seeking legal advice, and its contents do not represent an official position or decision by Ontario Health. It provides a series of questions and is not a finite resource and may not capture all considerations or circumstances; and in no event would following this sample guarantee acceptance of your solution by Ontario Health. Solution Providers should ensure that they fully read and understand the submission requirements and Terms and Conditions that govern the Virtual Visits Verification Program. If any discrepancy between this guide and the Virtual Visits Solution Requirements Version 2.1 (“Standard”) exists, then the Standard shall prevail.