HEALTH

MAY 2021

DIGITAL HEALTH UNDER *PHIPA*: SELECTED OVERVIEW

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

Disclaimer:

This guide by the Office of the Information and Privacy Commissioner of Ontario (IPC) is for informational purposes only and should not be relied upon as a substitute for the legislation itself, or as legal advice. It is intended to enhance understanding of rights and obligations under Ontario's access and privacy laws. It does not bind the IPC's Tribunal that may be called upon to independently investigate and decide upon an individual complaint or appeal based on the specific facts and unique circumstances of a given case. For the most up-to-date version of this guide, visit **www.ipc.on.ca**.

Contents

Introduction

Ontario's health privacy law, the *Personal Health Information Protection Act (PHIPA)*, governs how health information custodians (custodians) collect, use, disclose, retain, transfer, and dispose of personal health information. Since its inception, *PHIPA* has applied to personal health information in any form or medium that is in the custody or control of custodians.[1]

From time to time, *PHIPA* is amended to reflect changes in how health care is delivered. More and more, the delivery of health care relies on personal health information of individuals that is collected, stored, and accessed through electronic means by and between custodians. This guide provides custodians with an overview of various *PHIPA* provisions that have been adopted since February 2020 (some of which may not yet be in force) and that relate specifically to personal health information in digital format. They include:

- The Electronic Health Record
- Interoperability of digital health assets
- Electronic audit logs
- Consumer electronic service providers
- Access to records in electronic format

The Electronic Health Record

PHIPA's Part V.1 came into force on October 1, 2020. It governs a distinct record of digital personal health information known as the shared provincial electronic health record (EHR). This province-wide EHR is different from local electronic medical records or regional hospital information systems of custodians. Multiple custodians can contribute information to, and collect information from, the EHR, with no single custodian having custody or control of all of the information in the EHR.

Under Part V.1, the EHR is the electronic systems developed and maintained by the prescribed organization to enable custodians to collect, use, and disclose personal health information [s. 55.1(1)].[2] Ontario Health is the prescribed organization that, among other things, ensures the proper functioning of the EHR [s. 55.2(2)]. As such, Ontario Health has the power and duty to develop and maintain the EHR and is subject to the oversight mechanisms in Part V.1 [s. 55.2(1)].

This section of the guide summarizes the EHR-related responsibilities of custodians, Ontario Health and others under Part V.1 of *PHIPA*.

1) Collection, use, and disclosure by custodians

Given the unique EHR context, special definitions of collection, use, and disclosure by custodians apply [s. 55.1(2)]. For example, an individual first visits hospital A that contributes information about the individual to the EHR. The individual later visits hospital B that looks at the individual's record in the EHR. In this case:

- Hospital B ***collects*** personal health information the first time it views, handles, or deals with the information that was contributed to the EHR by hospital A [s. 55.1(2)(1)(i)].
- Hospital B ***uses*** personal health information any subsequent time it views, handles, or deals with the information that was contributed to the EHR by hospital A [s. 55.1(2)(1)(ii)].[3]
- Hospital A ***discloses*** personal health information only when hospital B collects the information from the EHR — ***not*** when hospital A first contributes the information to the EHR [s. 55.1(2)(3)].

Providing the information to Ontario Health for the purpose of contributing to the EHR is not considered to be a disclosure to — or a collection by — Ontario Health [s. 55.1(3)].

A custodian may collect an individual's personal health information by means of the EHR only for the purpose of providing or assisting in the delivery of health care to the individual, or if the custodian reasonably believes collection is necessary to eliminate or reduce a significant risk of serious bodily harm to the individual or others [s. 55.5(1)].

If a custodian has collected personal health information from the EHR for the purpose of providing or assisting in the delivery of health care to the individual, the custodian can then use or disclose the information for any purpose permitted or required by *PHIPA* [s. 55.5(4)]. If a custodian has collected personal health information from the EHR for the purpose of eliminating or reducing a significant risk of serious bodily harm, the custodian may only use or disclose the information for that purpose [s. 55.5(5)].

2) Consent directives

Withholding or withdrawing consent

Individuals cannot opt out of having their personal health information included in the EHR, but they have the right to make a consent directive. A consent directive occurs when an individual withholds or withdraws, in whole or in part,[4] their consent to the collection, use, and disclosure of their personal health information by a custodian for health care purposes [s. 55.6(1)]. Individuals may also withdraw or modify their consent directives [s. 55.6(3)].

Ontario Health is responsible for implementing consent directives with respect to personal health information in the EHR [s. 55.6(2)]. For example, Ontario Health is responsible for notifying a custodian if information being sought by the custodian is subject to a consent directive [s. 55.6(7)]. Ontario Health is also responsible for ensuring that consent directives made before October 1, 2020, continue to be in place [O. Reg. 329/04, s. 18.5(1)].[5]

Restrictions

A consent directive cannot apply to basic demographic information such as the individual's name, date of birth, or Ontario health card number [O. Reg. 329/04, s. 18.4(4)]. Additionally, despite any consent directive, Ontario Health can utilize personal health information in the EHR to provide alerts to custodians about potentially harmful medication interactions, as long as the alerts do not reveal the substance of the personal health information that is subject to the consent directive [s. 55.8].

Consent overrides

In certain circumstances, custodians are permitted to collect personal health information from the EHR despite a consent directive. This is known as a consent override [s. 55.7]. Consent overrides are permitted when:

- the individual gives express consent for the custodian to collect their personal health information despite a consent directive indicating otherwise [s. 55.7(1)];
- the custodian seeking to collect personal health information that is the subject of a consent directive reasonably believes that it is necessary for eliminating or reducing a significant risk of serious bodily harm to the individual *and* it is not reasonably possible to get the individual's timely consent [s. 55.7(2)]; or
- the custodian seeking to collect personal health information that is the subject of a consent directive reasonably believes that it is necessary for eliminating or reducing a significant risk of serious bodily harm to another person or group of persons [s. 55.7(3)].

In each of these three circumstances, the custodian collecting the personal health information from the EHR may only use or disclose it for the purpose for which it is being collected [s. 55.7(4)].

Ontario Health must audit and monitor every instance in which a consent override takes place [s. 55.7(5)].

Notifications

When a consent override occurs, two notifications must happen:

- Ontario Health must immediately notify the custodian that collected the information from the EHR despite the consent directive [s. 55.7(6)]. This notification to the custodian is required because it may have been an agent of the custodian, not the custodian itself, that collected the information.
- The custodian that collected the information from the EHR despite the consent directive must notify the individual who made the consent directive at the first reasonable opportunity [s. 55.7(7)(a)].

There is an additional notice requirement if the consent override occurred to eliminate or reduce a significant risk of bodily harm to another person or group of persons:

- The custodian that collected the information from the EHR despite the consent directive must also notify the IPC at the first reasonable opportunity [s. 55.7(7)(b)].

In providing this notice to the IPC, the custodian must not include identifying information about the individual or the person or group of persons at risk of harm [s. 55.7(7)(b)]. Similarly, in providing notice to the individual of a consent override for the purpose of eliminating or reducing a significant risk of bodily harm to another person or group of persons, the custodian must not include identifying information about the person or group of persons at risk of harm [s. 55.7(8)].

Additional requirements relating to the content of notifications of consent overrides are set out in the regulations to *PHIPA* [O. Reg. 329/04, ss. 18.6, 18.7, and 18.8].

3) Privacy breaches

PHIPA imposes a general duty on custodians to protect personal health information against privacy breaches,[6] and to notify individuals (and, in some circumstances, the IPC) if a privacy breach occurs [s. 12]. For more information on responding to health privacy breaches, see the IPC's **Responding to a Health Privacy Breach: Guidelines for the Health Sector**.

If personal health information is collected without authority in the particular context of the EHR:

- The custodian responsible for the unauthorized collection must notify the individual and inform them of their right to complain to the IPC [s. 55.5(7)(a)].
- In certain circumstances, which are set out in the regulations, the same custodian must also notify the IPC [s. 55.5(7)(b)].[7]
- The same custodian must include, in its annual reporting of privacy breach statistics to the IPC, the number of times personal health information was collected by the custodian by means of the EHR without authority [O. Reg. 329/04, s. 6.4(1)(5)]. For more information on annual reporting, see the IPC's **Annual Reporting of Privacy Breach Statistics to the Commissioner: Requirements for the Health Sector**.[8]

For Ontario Health's part, if personal health information is stolen or lost, or if it is collected, used, or disclosed without authority, Ontario Health must notify at the first reasonable opportunity any custodian that provided that information to Ontario Health [s. 55.3(11)]. Ontario Health must also immediately notify the IPC if Ontario Health (or someone acting on its behalf) views, handles, deals with, makes available, or releases personal health information in the EHR other than in accordance with *PHIPA* or its regulations [s. 55.3(15)].

Part V.1 provides some protection from liability for custodians that, acting in good faith, contributed personal health information to the EHR. Such custodians are not liable for damages if Ontario Health or those acting on its behalf view, handle, or otherwise deal with personal health information in the EHR in an unauthorized manner or if any other custodian collects information in the EHR in an unauthorized manner [s. 55.13].

4) Responsibilities of Ontario Health as the prescribed organization

Ontario Health's major functions with respect to the EHR include:

- managing and integrating the personal health information it receives from custodians
- ensuring the proper functioning of the EHR
- ensuring the accuracy and quality of the information in the EHR
- analyzing information in the EHR in order to provide alerts and reminders to custodians for use in the provision of health care [s. 55.2(2)]

Part V.1 also contains specific requirements Ontario Health must meet as it develops and maintains the EHR.

Transparency

Ontario Health must make available to the public, and each custodian contributing personal health information to the EHR, a plain language description of the EHR, including a general description of the administrative, technical, and physical safeguards in place to protect personal health information [s. 55.3(3)(i)]. Ontario Health must also make its EHR-related directives, guidelines, or policies available to the public and custodians [s. 55.3(3)(ii)].[9]

Logging, auditing, and monitoring

Ontario Health must log, audit, and monitor instances where personal health information in the EHR is viewed, handled, or otherwise dealt with [s. 55.3(4)(i)].[10] Ontario Health must also log, audit, and monitor instances where consent directives are made, withdrawn, modified, or overridden [s. 55.3(5) and (6)].

If a custodian requires these logs to audit and monitor its own compliance with *PHIPA* and requests these logs, Ontario Health must provide them to the custodian [s. 55.3(9)].

Privacy and security assessments

For each system retrieving, processing, or integrating personal health information in the EHR, Ontario Health must perform an assessment of threats, vulnerabilities, and risks to the security and integrity of the personal health information and how the system may affect the privacy of individuals [s. 55.3(10)]. Ontario Health must make the results of these assessments available to custodians that have contributed personal health information to the EHR to which these assessments relate [s. 55.3(12)(i)]. Ontario Health must also provide a summary of the results to the public [s. 55.3(12)(ii)].

Individuals' access and correction requests

Ontario Health must have in place and comply with practices and procedures approved by the Minister of Health for responding to requests by individuals to access or correct their records of personal health information in the EHR [s. 55.3(18)]. The specific provisions in *PHIPA* about access and correction as they relate to Ontario Health and the EHR have not yet been proclaimed into force [s. 51(5) and (6)].

5) Oversight of Ontario Health

Ontario Health must comply with any directives from the Minister of Health [s. 55.4(1)].

An advisory committee will be established with the role of making recommendations to the Minister of Health concerning:

- Ontario Health's practices and procedures — including administrative, technical, and physical safeguards — to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of the information [s. 55.11(1)(a) and (c)]
- Ontario Health's practices and procedures to respond to access or correction requests [s. 55.11(1)(b)]
- Privacy breach notice obligations and Ontario Health's role in assisting custodians in fulfilling their notice obligations to individuals [s. 55.11(1)(d) and (e)]
- Anything that Part V.1 of *PHIPA* or its regulations refer to as capable of being the subject of a recommendation of the advisory committee [s. 55.11(1)(f)]
- Any other matter the Minister of Health refers to the advisory committee [s. 55.11(1)(g)]

Ontario Health must have practices and procedures in place for protecting the privacy of the individuals whose personal health information it receives and for maintaining the confidentiality of the information [s. 55.3(14)].

The IPC is responsible for reviewing (and approving, at its discretion) Ontario Health's practices and procedures within one year of Part V.1 coming in force and every three years thereafter [s. 55.3(14) and s. 55.12].

At any time, the IPC can request to view the logs that Ontario Health is required to keep under Part V.1 [s. 55.3(8)].[11] Ontario Health must also submit to the IPC, at least on an annual basis, a report about consent overrides that have occurred since the last report [s. 55.3(16)].

The IPC must be consulted on directives made by the Minister of Health to Ontario Health regarding the EHR [s. 55.4(2)].

Finally, the IPC can receive complaints relating to any provision of *PHIPA* and its regulations, including complaints relating to the EHR [s. 56].

6) Providing certain entities to access personal health information in the EHR

There are a number of provisions in Part V.1 of *PHIPA* that allow certain entities to access personal health information in the EHR for specific purposes.

The Ministry of Health's data integration unit

Part III.1 of the ***Freedom of Information and Protection of Privacy Act*** *(FIPPA)* contains a framework that permits designated units, including "ministry data integration units," to collect and combine personal information from different sources for the purposes of analysis of government programs and services and the management of resources. The Ontario Ministry of Health's Capacity Planning and Analytics Division is designated as a ministry data integration unit [O. Reg. 366/19, s. 2(4)]. This unit may collect personal health information from the EHR for the purposes of, and in accordance with the requirements set out in, *FIPPA*'s data integration framework [s. 55.9].

Coroners

Ontario Health may provide personal health information in the EHR to a coroner for an investigation conducted under the ***Coroners Act*** [s. 55.9.1(1)]. In such circumstances, the coroner and Ontario Health would be obligated to comply with specific requirements set out in the regulations to *PHIPA* [O. Reg. 329/04, ss. 18.10 and 18.11].

Medical officers of health

The Chief Medical Officer of Health for the province of Ontario, as well as the medical officers of each public health unit in Ontario, may collect personal health information from the EHR for the purposes of administering the ***Health Protection and Promotion Act*** or the ***Immunization of School Pupils Act*** [s. 55.9.1(2)].

As directed by the Minister of Health for purposes other than health care

The Minister of Health may direct the disclosure of personal health information in the EHR to:

- prescribed persons to compile or maintain a registry to facilitate or improve health care or that relates to the storage or donation of body parts or bodily substances[12]
- prescribed entities to analyze or compile statistics in planning and managing the health care system[13]
- certain public health authorities for purposes of the ***Health Protection and Promotion Act*** or the ***Immunization of School Pupils Act*** and to similar public health authorities federally, in other provinces or territories, or internationally for a purpose that is substantially similar to a purpose of one of those acts
- Public Health Ontario for purposes of the ***Ontario Agency for Health Protection and Promotion Act, 2007***
- a researcher conducting research in compliance with *PHIPA* [s. 55.10(1)]

In issuing such directives, the Minister of Health must not:

- direct the disclosure of personal health information in the EHR if other information will serve the same purpose [s. 55.10(5)]

- direct the disclosure of more personal health information than is reasonably necessary to meet the purpose of the disclosure [s. 55.10(6)]

The minister must also consult with the advisory committee prior to directing any of these disclosures [s. 55.10(1)(c)].

Interoperability of digital health assets

The exchange of information between the various electronic systems of different custodians is important for delivering health care in an efficient, integrated manner. In addition to amendments to address the EHR, *PHIPA* was recently amended to allow regulations to be made governing interoperability between the individual electronic systems of custodians [s. 73(1)(n.5)]. These regulations came into force on January 1, 2021 [O. Reg. 329/04, ss. 26 - 34].

Under these regulations, Ontario Health[14] is responsible for specifying the ways in which "digital health assets" of custodians must be interoperable with one another [O. Reg. 329/04, s. 27(1)]. A digital health asset is a product or service that is selected, developed, or used by a custodian and enables them to use electronic means to collect, use, modify, disclose, transmit, retain, or dispose of personal health information to provide health care or assist in the delivery of health care [O. Reg. 329/04, s. 26]

An interoperability specification may include (but is not limited to) a requirement related to:

- the content of data or a common data set for electronic data
- the format or structure of messages exchanged between digital health assets
- the migration, translation, or mapping of data from one digital health asset to another
- terminology, including vocabulary, code sets, or classification systems
- privacy or security [O. Reg. 329/04, s. 26]

An interoperability specification must describe certain prescribed elements such as the names or classes of custodians or the types of digital health assets to which it applies, the date it becomes effective, and any applicable exemptions [O. Reg. 329/04, s. 28(2)].

An interoperability specification may be either general or specific in its application and may be limited to a custodian's selection, development, or use of particular digital health assets or classes of digital health assets [O. Reg. 329/04, s. 28(1)].

1) Minister of Health

The Minister of Health reviews and approves interoperability specifications and may direct Ontario Health to establish or amend interoperability specifications [O. Reg. 329/04, s. 27(3)].

The Minister of Health must consult with Ontario Health before issuing a direction to establish or amend particular interoperability specifications in respect of certain matters [O. Reg. 329/04, s. 27(4)].

Interoperability specifications do not take effect unless they have been approved by the Minister of Health [O. Reg. 329/04, s. 27(1)].

2) Ontario Health

Ontario Health establishes, maintains, and amends interoperability specifications in consultation with any stakeholder(s) it considers appropriate [O. Reg. 329/04, s. 27(1) and (2)]. Ontario Health may be directed to establish or amend interoperability specifications by the Minister of Health [O. Reg. 329/04, s. 27(3)]. If the minister issues such direction, Ontario Health must comply [O. Reg. 329/04, s. 27(5)].

Ontario Health must:

- make the interoperability specifications public [O. Reg. 329/04, s. 29]
- establish a process for certifying digital health assets that are compliant with the interoperability specifications and make a list of certified digital health assets public [O. Reg. 329/04, s. 31]
- monitor custodians' compliance with the requirement to ensure that their selection, development, or use of digital health assets complies with applicable interoperability specifications [O. Reg. 329/04, s. 33][15]

Ontario Health may make a complaint to the IPC where there are reasonable grounds to believe that a custodian has selected, developed, or used a digital health asset that does not comply with an interoperability specification, or is about to do so [O. Reg. 329/04, s. 34].

3) Custodians

Custodians must ensure that every digital health asset they select, develop, or use complies with applicable interoperability specifications [O. Reg. 329/04, s. 30(1)]. However, selecting, developing, or using a compliant digital health asset does not relieve a custodian of its obligation to comply with other provisions of *PHIPA* and its regulations [O. Reg. 329/04, s. 30(2)].

Custodians should be aware of the interoperability specifications that are in effect and which digital health assets have been certified as being compliant with the interoperability specifications. The specifications may be amended from time to time.

Custodians must cooperate with Ontario Health in monitoring compliance with applicable specifications [O. Reg. 329/04, s. 33(2)]. Custodians must also provide reports to Ontario Health upon request on their compliance with the requirement to select, develop, or use digital health assets that comply with the applicable specifications [O. Reg. 329/04, s. 32]. Information, records, and reports provided by custodians to Ontario Health must not include personal health information [O. Reg. 329/04, ss. 32(3) and 33(3)].

4) The IPC

When establishing or amending an interoperability specification relating to the confidentiality of personal health information, the privacy of individuals, or the rights of individuals to access or correct records of their personal health information, Ontario Health must consult with, and consider any recommendations made by, the IPC [O. Reg. 329/04, s. 27(6)].

The IPC may receive complaints (including from Ontario Health) about non-compliance with the interoperability specifications [s. 56; O. Reg. 329/04, s. 34].

Electronic audit logs

As the IPC has stated in its guidance on **Detecting and Deterring Unauthorized Access to Personal Health Information**, the logging, auditing, and monitoring of all accesses to electronic records of personal health information is important to protect the privacy of individuals and the confidentiality of their personal health information. This flows from a custodian's obligation to protect personal health information from, among other things, theft, loss, and unauthorized use and disclosure.

PHIPA now contains a section (not yet in force) that specifically requires custodians that use electronic means to collect, use, disclose, modify, retain, or dispose of personal health information to maintain an electronic audit log, subject to any prescribed exceptions [s. 10.1]. This log must audit and monitor every instance in which an electronic record of personal health information is viewed, handled, modified, or otherwise dealt with [s. 10.1(4)].

The electronic audit log must include:

- the type of personal health information viewed, handled, modified, or dealt with
- the date and time the information was viewed, handled, modified, or dealt with
- the identity of all persons who viewed, handled, modified, or dealt with the personal health information
- the identity of the individual to whom the personal health information relates
- any other information that may be required by the regulations [ss. 10.1(4)(a) to (e)]

At any time, the IPC may request a copy of the electronic audit log that the custodian must provide, even if it contains personal health information [s. 10.1(2) and (3)].

Consumer electronic service providers

PHIPA contains provisions (not yet in force) governing "consumer electronic service providers" [s. 54.1]. A consumer electronic service provider delivers electronic services to individuals at their request, primarily for the purpose of allowing those individuals to access, use, disclose, modify, maintain, or otherwise manage their records of personal health information or other prescribed purposes [s. 54.1(1)]. For example, an individual might use a smartphone app to store information about their blood sugar levels or to view their laboratory test results.

Regulations may be made under *PHIPA*[16] governing the services of consumer electronic service providers [s. 73(1)(m.1)]. For example, regulations may be made about their collection, use, and disclosure of personal health information, the use of their services by custodians and individuals, and the rights of individuals with regard to their services. The consumer electronic service provider may, if authorized by the individual, collect and use the individual's Ontario health card number — in accordance with any rules to be set out in the regulations — in order to verify the individual's identity or for any other prescribed purpose [s. 54.1(3)].

A custodian providing personal health information to a consumer electronic service provider must comply with any applicable requirements or procedures contained in the regulations [s. 54.1(4)]. If a custodian receives an individual's access request from a consumer electronic service provider, the custodian is not obligated to provide personal health information to the consumer electronic service provider in response [s. 54.1(5)].

The IPC's order-making powers include the power to require a custodian or class of custodians to stop providing personal health information to a consumer electronic service provider [s. 61(1)(f.1)].

Access to records in electronic format

Individuals have the right to access their records of personal health information in the custody or control of custodians, subject to limited exceptions [s. 52]. This right of access now includes the right to obtain access to the record in an electronic format that meets prescribed requirements [s. 52(1.1)]. These requirements have yet to be prescribed.

This expanded right is important given the accelerating digitization of records and the increasing interest of individuals to access these records in electronic format through patient portals or in a manner compatible for use with health apps or other platforms.

For more information about access under *PHIPA*, see the IPC's ***PHIPA* Practice Direction #2: Responding to a Request for Access to Personal Health Information**, and the section about access and correction of records in the IPC's **Frequently Asked Questions: Personal Health Information Protection Act**.

End notes

1 Note that, in specific circumstances, *PHIPA* also regulates personal health information that is not in the custody or control of health information custodians.

2 In this guide, all section numbers are references to *PHIPA* unless noted otherwise.

3 If hospital B itself further contributes personal health information about the individual to the EHR, hospital B is using this information every time it views, handles, or deals with this information [s. 55.1(2)(2)].

4 A consent directive made on or after October 1, 2020 applies to all of the individual's personal health information that is accessible by means of the EHR, unless it is reasonably possible for Ontario Health to apply the consent directive only to the information that has been specified by the individual, in which case the consent directive applies only to that information [O. Reg. 329/04, s. 18.4(3)].

5 Unless the individual subsequently made a consent directive on or after October 1, 2020, in which case Ontario Health must implement the later directive [O. Reg. 329/04, s. 18.5(2)].

6 Part V.1 provides that if Ontario Health transmits personal health information to a custodian by means of the EHR at the custodian's request, the custodian has a duty to protect that information against privacy breaches, regardless of whether the custodian has viewed, handled, or otherwise dealt with the information [s. 55.5(6)].

7 The circumstances in which the IPC must be notified of an unauthorized collection in the EHR context are the same as the circumstances in which the IPC must be notified of an unauthorized use or disclosure in the non-EHR context [O. Reg. 329/04, s. 18.3(1)]. These circumstances are explained in the IPC's **Reporting a Privacy Breach to the IPC: Guidelines for the Health Sector**.

8 The disclosing custodian that contributed the personal health information to the EHR in the first place is not required to include unauthorized disclosures by means of the EHR in its annual report to the IPC [O. Reg. 329/04, s. 6.4(3)].

9 To the extent that these do not reveal a trade secret or confidential scientific, technical, commercial, or labour relations information.

10 Or is transmitted to a custodian at the custodian's request [s. 55.3(4)(ii)].

11 These logs are described in *PHIPA* section 55.3, paragraph 4 (instances where personal health information in the EHR is viewed, handled, or otherwise dealt with, or is transmitted to a custodian at the custodian's request), paragraph 5 (consent directives), and paragraph 6 (consent overrides).

12 The prescribed persons are Cardiac Care Network of Ontario in respect of its registry of cardiac and vascular services, INSCYTE (Information System for Cytology etc.) Corporation in respect of CytoBase, Hamilton Health Sciences Corporation in respect of the Critical Care Information System, Ontario Health in respect of the Ontario Cancer Screening Registry, Children's Hospital of Eastern Ontario — Ottawa Children's Treatment Centre in respect of the Better Outcomes Registry and Network, and Ontario Institute for Cancer Research in respect of the Ontario Tumour Bank [O. Reg. 329/04, s. 13(1)].

13 The prescribed entities are Canadian Institute for Health Information, Institute for Clinical Evaluative Sciences, Pediatric Oncology Group of Ontario, and Ontario Health [O. Reg. 329/04, s. 18(1)].

14 Ontario Health's responsibility for establishing interoperability specifications is separate from its duties as the prescribed organization for the EHR. Interoperability specifications may apply to any digital health asset.

15 Ontario Health must develop a process for monitoring compliance [O. Reg. 329/04, s. 33(1)]. This monitoring may include consulting with custodians on how compliance may be achieved [O. Reg. 329/04, s. 33(4)]. Ontario Health may also request that a custodian submit a report on its compliance [O. Reg. 329/04, s. 32(1)]. Upon receipt of the report, Ontario Health must determine whether the custodian is in compliance and advise the custodian of its determination [O. Reg. 329/04, s. 32(4)].

16 When the relevant regulation-making authority comes into force.

Digital Health under *PHIPA*: Selected Overview

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

2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada M4W 1A8
Phone: (416) 326-3333 / 1-800-387-0073

www.ipc.on.ca
info@ipc.on.ca

May 2021