REPORT OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

OCTOBER 1, 2021

Review of Ontario Health: The Prescribed Organization under the *Personal Health Information Protection Act*

Information and Privacy Commissioner of Ontario

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

CONTENTS

Introduction

The *Personal Health Information Protection Act, 2004* (*PHIPA* or the *Act*) establishes rules for the collection, use and disclosure of personal health information by health information custodians, that protect the privacy of individuals and the confidentiality of their personal health information.

Prescribed organizations have the power and duty to develop and maintain the electronic health record (EHR) for the province in accordance with Part V.1 of *PHIPA* and Ontario Regulation 329/04 (the regulation). Part V.1 of *PHIPA*, which sets out the requirements related to the EHR, came into force on October 1, 2020. At the same time, Ontario Health was prescribed under section 18.1 of the regulation as the organization for the purposes of Part V.1 of *PHIPA*.

As the oversight body responsible for ensuring compliance with *PHIPA*, the Information and Privacy Commissioner of Ontario (IPC) must review and approve the practices and procedures of the prescribed organization within one year of Part V.1 of *PHIPA* coming into force and, thereafter, every three years.

This report summarizes the IPC's initial review of Ontario Health's policies, practices and procedures as a prescribed organization for the purposes of Part V.1 of *PHIPA*.

About Ontario Health

In 2019, the *Connecting Care Act, 2019 (CCA)* created a single agency, Ontario Health, to assume centralized responsibilities for 21 pre-existing agencies. At the time of the writing of this report, the below agencies and their operations have been transferred to Ontario Health through transfer orders issued by the Minister of Health:

- Trillium Gift of Life Network
- Ontario Telemedicine Network
- Cancer Care Ontario
- eHealth Ontario
- HealthForceOntario Marketing and Recruitment Agency
- Health Quality Ontario
- Health Shared Services Ontario
- Parts of the following Local Health Integration Networks (LHINs)
    - Central LHIN
    - Central East LHIN
    - Central West LHIN
    - Champlain LHIN
    - Erie St. Clair LHIN
    - Hamilton Niagara Haldimand Brant LHIN
    - Mississauga Halton LHIN
    - South East LHIN
    - South West LHIN
    - Toronto Central LHIN
    - Waterloo Wellington LHIN
    - North East LHIN
    - North Simcoe Muskoka LHIN
    - North West LHIN
- Cardiac Care Network of Ontario (CorHealth) – *transfer pending*

According to the Ministry of Health's website as of the date of this report,[1] once fully established, Ontario Health is expected to integrate the following key responsibilities:

System Management and Performance

- overseeing the delivery of health care
- improving the quality of care
- measuring and managing how the system performs
- enabling innovation
- ensuring financial accountability
- providing clinical leadership

Population–Based Programs and Clinical and Quality Standards

- overseeing highly specialized care (for example: cancer, organ donation)
- managing provincial population health programs (for example: cancer screening)
- investigating and supporting new and emerging health services
- developing evidence-based advice for delivering health services and clinical care

Back Office Support

- accountability for an integrated supply chain for health care products and services
- shared information technology resources

System oversight

- assessing and planning for local needs
- holding accountability for Ontario Health Teams in the future

Ontario Health as the Prescribed Organization

As the prescribed organization, Ontario Health is mandated by *PHIPA* to perform the following functions:

1. Manage and integrate the personal health information it receives from health information custodians.
2. Ensure the proper functioning of the EHR by servicing the electronic systems that support the EHR.
3. Ensure the accuracy and quality of the personal health information that is accessible by means of the EHR by conducting data quality assurance activities on the personal health information it receives from health information custodians.
4. Conduct analyses of the personal health information that is accessible by means of the EHR in order to provide alerts and reminders to health information custodians for their use in the provision of health care to individuals.

Paragraph 14 of section 55.3 of *PHIPA* sets out that on and after the first anniversary of that section coming into force, Ontario Health, as the prescribed organization, must have in place, and comply with, practices and procedures that are approved by the IPC.

1 https://www.ontario.ca/page/ontario-health-agency

Ontario Health's Other Prescribed Status and Roles under *PHIPA*

Ontario Health has a number of other functions and roles under *PHIPA*. The review of Ontario Health described in this report is only of Ontario Health's functions as the prescribed organization in respect of the development and maintenance of the EHR pursuant to Part V.1 of *PHIPA*, and not any of its other functions.

In addition to its role as the prescribed organization pursuant to Part V.1 of *PHIPA*, Ontario Health has assumed the mandates of other agencies that have prescribed roles under *PHIPA*, and in those capacities must also have their practices and procedures reviewed and approved by the IPC every three years:

Prescribed entity

Health information custodians are permitted, pursuant to section 45 of *PHIPA*, to disclose personal health information to a prescribed entity for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services.

Ontario Health has assumed the functions that were carried out by Cancer Care Ontario as a prescribed entity.

Prescribed person in respect of the Ontario Cancer Screening Registry

Health information custodians are permitted, pursuant to section 39 (1) (c) of *PHIPA*, to disclose personal health information to a prescribed person for the purpose of compiling and maintaining a registry of personal health information for the purposes of facilitating or improving the provision of health care or as related to the storage or donation of body parts or bodily substances.

Ontario Health is currently a prescribed person in respect of the Ontario Cancer Screening Registry that was also transferred as part of Cancer Care Ontario.

Prescribed person in respect of the registry of cardiac and vascular services

As of January 1, 2021, the Cardiac Care Network of Ontario (CorHealth) was prescribed as an organization to be transferred to Ontario Health, pursuant to the transfer order powers under section 40 of the *CCA*. The transfer order is anticipated to be issued later this year. This will result in an additional prescribed status for Ontario Health as a prescribed person in respect of the registry of cardiac and vascular services that has been compiled and maintained by CorHealth.

Ontario Health also operates under other authorities under *PHIPA*. Ontario Health must comply with additional requirements set out in *PHIPA* and the regulation related to these roles:

Electronic service provider

As an electronic service provider (ESP), Ontario Health supplies services for the purpose of enabling health information custodians to collect, use, modify, disclose, retain or dispose of personal health information electronically. There are a number of obligations set out under section 6 of the regulation to *PHIPA* for ESPs that are not agents.

Health information network provider

Health information network providers (HINPs) are a specific type of ESP described under section 6 of the regulation to *PHIPA*. Ontario Health acts as a HINP when it provides services to two or more health information custodians where the services are provided primarily to health information custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not Ontario Health is an agent of any of the health information custodians.

Researcher

Ontario Health may also act as a researcher under section 44 of *PHIPA*. A researcher is a person who conducts systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of them, and includes the development, testing and evaluation of research. Researchers who receive personal health information from health information custodians must comply with the obligations set out under *PHIPA* and its regulation.

Agent

Ontario Health may also act as an agent of a health information custodian pursuant to s.17 of *PHIPA*. For example, Ontario Health may act as an agent by providing custodians with the secure storage for repositories containing health information custodians. In its role as an agent, Ontario Health acts on behalf of a health information custodian and not for Ontario Health's own purposes, and may only collect, use, disclose, retain or dispose of personal health information if the health information custodian is permitted or required to do so.

Agency responsible for interoperability specifications

Pursuant to sections (26)-(34) of the *PHIPA* regulation, Ontario Health is the agency responsible for establishing, maintaining and amending interoperability specifications. These are business or technical requirements that apply to digital health assets and may include requirements 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,
- The terminology, including vocabulary, code sets or classification systems, or
- Privacy or security.

Three-Year Review and Approval Process

The *Manual for the Review and Approval of Prescribed Organizations* (the "Manual") outlines the process that will be followed by the IPC in reviewing the practices and procedures put in place by the prescribed organization and describes the requirements that must be met for approval.

The requirements are based on an assessment of what would constitute a reasonable combination of practices and procedures. What is "reasonable" is based on the nature of the functions performed by the prescribed organization, the amount and sensitivity of the personal health information received for the

purpose of developing and maintaining the EHR, the number and nature of the individuals with access to the personal health information, as well as the obligations and duties of the prescribed organization under *PHIPA* and its regulation.

The process followed by the IPC in conducting its review depends on whether the review relates to the initial review of the practices and procedures put in place by the prescribed organization, or the ongoing review of these practices and procedures every three years from the date of the previous approval.

Initial Review and Approval

The first time the IPC reviews and approves the practices and procedures of the prescribed organization, all of the organization's relevant policies, practices and procedures that establish the organization's compliance with the Manual are reviewed. Through an iterative review process, the IPC provides the prescribed organization with comments and the prescribed organization submits revisions to address those comments. Additional documentation and clarifications may be required over the course of the review.

Once all revisions and any additional documentation and necessary clarifications are received, an on-site meeting would typically be scheduled between the IPC and representatives of the prescribed organization. The purpose of the on-site meeting is to discuss the practices and procedures put in place by the prescribed organization, and to provide the IPC with an opportunity to review first-hand certain physical security measures put in place to protect personal health information.

Following the on-site meeting, the IPC provides any additional comments and feedback regarding its practices and procedures and compliance with the Manual. Once the prescribed organization has responded to this feedback, the IPC prepares a draft report and submits the report to the prescribed organization for review and comment.

When the report is finalized, it is posted on the IPC's website, along with a letter of approval. The report and letter of approval are also required to be posted on the website of the prescribed organization.

The final report and letter of approval may contain recommendations in respect of the practices and procedures put in place by the prescribed organization. The IPC expects the prescribed organization to comply with the recommendations on or before the deadline set out in the final report or letter of approval.

Subsequent Triennial Review and Approval

Review of the practices and procedures of the prescribed organization by the IPC is required every three years from the date of the initial approval.

A subsequent review would typically begin two years following the date of the prior approval (one year prior to the end of the three year review cycle). This allows IPC staff and the prescribed organization one year to engage in an iterative discussion process and provides the prescribed organization an opportunity to address any issues in advance of the required approval.

The next three-year review period of Ontario Health as a prescribed entity and prescribed person will begin on November 1, 2022 with an approval date of October 31, 2023. For practical purposes, and by mutual agreement between the IPC and Ontario Health, this initial approval of Ontario Health as the prescribed organization in respect of Part V.1 of *PHIPA* will likewise end on October 31, 2023 to coincide cyclically with these other reviews.

Review of the Prescribed Organization

Documents Reviewed

Below is a description of the documents reviewed by the IPC and their submission dates. Some titles of documentation changed over the course of the review. For clarity, only the final titles are described.

Privacy Documentation

Initially received April 1, 2021:

- *EHR Consent Directive and Consent Override Policy*
- *EHR Consent Directive Request Form*
- *EHR Inquiries and Complaints Policy and Procedures*
- *EHR Plain Language Description and List of Repositories that are Accessible by the EHR*
- *EHR Policy for Receiving Personal Health Information*
- *EHR Privacy Incident Management Policy and Procedure*
- *EHR Request for Access and Correction Form*
- *EHR Request for Access to Personal Health Information Policy and Procedure*
- *EHR Request for Correction to Personal Health Information Policy and Procedure*
- *EHR Retention Policy and Procedure*
- *EHR Statement of Information Practices*
- *Ontario Health Privacy Complaint Form*
- *Privacy Policy*
- *Policy Governance Framework*
- *Privacy Audit and Compliance Policy*
- *Privacy Complaints and Inquiries Policy and Procedures*
- *Privacy Governance and Accountability Framework*
- *Privacy Impact Assessment Standard*
- *Privacy Incident Management Policy and Procedure*
- *Privacy Transparency Policy*
- *Privacy Use and Disclosure Policy*

Initially received June 1, 2021:

- *Schedule for Privacy, Security and Confidentiality for Third Party Service Provider Agreements*

Initially received July 2, 2021:

- *Privilege Access Management Procedure*
- *Process for Tracking Third Party Service Provider that are Permitted to Use Personal Health Information or Personal Information*

Security Documentation

Initially received May 1, 2021:

- *Acceptable Use Agreement for Ontario Health Employees and Other Agents Template*
- *Access Card Procedure*
- *Access Control Standard*
- *Cryptography Standard*

- *EHR Policy and Procedures for Agreements with Health Information Custodians and Coroners*
- *EHR Privacy Auditing and Monitoring Policy*
- *External Information Security Incident Management Standard*
- *Hard Copy Personal Health Information/Personal Information and Media Destruction Procedure*
- *Information Classification and Handling Guideline*
- *Information Classification and Handling Standard*
- *Information Security Acceptable Use Policy*
- *Information Security Incident Management Standard*
- *Information Security Operations Standard*
- *Information Security Policy*
- *Information Security Program Governance*
- *Information Security Risk Management Standard*
- *Media Destruction, Sanitization and Disposal Standard*
- *Mobile Security Standard*
- *Network Security and Communications Standard*
- *Personal Health Information Handling Standard*
- *Physical Access Policy*
- *Physical and Environmental Security Standard*
- *Privacy Notices Policy and Procedure*
- *Secure Transfer of Sensitive Information Standard*
- *Visitor Access Procedure*

Initially received July 16, 2021:

- *Exchanging Personal Health Information via Application Services Procedure*
- *Exchanging Personal Health Information via Managed File Transfer Procedure*
- *Security Definitions Master Sheet*

Initially received August 13, 2021:

- *Cyber Security Incident Response Process*

Initially received August 16, 2021:

- *Ministry of Government and Consumer Services (MGCS) Data Centre Operations Physical Security Access Control Policy and Procedures Guide*
- *Government of Ontario IT Standard (GO-ITS) Physical Security Requirements for Data Centres*

Initially received August 20, 2021:

- *Restricted Access at 777 Bay Street Guide*

Initially received August 24, 2021:

- *EHR Access Services Schedule*
- *Registration and Sponsorship Schedule*
- *Services Agreement*

Initially received September 1, 2021:

- Walkthrough of Restricted Access – *777 Bay Guide* (presentation)

Human Resources Documentation

Initially received June 1, 2021:

- *Chief Privacy Officer Job Description*
- *Confidentiality Agreements Policy*
- *Director, Enterprise Information Security Office Job Description*
- *Legacy Termination of Employment Access and Return of Assets Procedures*
- *Mandatory Training Standard*
- *Privacy and Security Training and Awareness Policy and Procedure*
- *Progressive Discipline Policy*
- *Statement of Confidentiality for Ontario Health Employees and Other Agents Template*
- *Termination of Employment Policy*
- *Vice President, Innovations for Connected Health – Job Description*

Initially received July 9, 2021:

- *Confidentiality Agreements Template*
- *Digital Leads Table Terms of Reference*

Initially received July 23, 2021:

- *Digital Excellence in Health – Cyber Security Steering Committee Terms of Reference*

Organizational and Other Documentation

Initially received June 1, 2021:

- *Crisis Management Operating Standard*
- *Digital Work Stream – Cyber Security Working Group Terms of Reference*
- *Enterprise Risk Management and Governance Framework*
- *Enterprise Risk Management Policy*
- *Governance Model: Connecting Security Committee Terms of Reference*
- *Innovation and Transformation Committee Terms of Reference*
- *IT Service Continuity Management 101 Transcript*
- *ITSCM 101: Advisory & Awareness Course – IT Service Continuity Plan Ontario Health Terms of Reference: Innovation and Transformation Committee*
- *ONE Support – IT Incident Management Policy*
- *ONE Support – IT Incident Management Process and Procedures Guide*
- *ONE Support – IT Major Incident Procedures Guide*
- *Ontario Health Business Continuity Plan Template*
- *Privacy Program Advisory Committee Terms of Reference*
- *Privacy and Security Log of Recommendations Standard*
- *Privacy Governance and Accountability Framework*
- *Privacy Program Advisory Committee Terms of Reference*
- *Privacy Risk Management Policy and Procedures*

Initially received August 16, 2021:

- *Enterprise Risk Management Oversight Committee Terms of Reference*

Initially received September 15, 2021:

- *Integrated Project Plan: Ontario Health Business Continuity and Disaster Recovery Initiative*

Indicators

Initially received July 2, 2021:

- *Security Indicators (except those related to security breaches)*
- *Human Resources Indicators*
- *Organizational and Other Indicators*

Initially received July 7, 2021:

- *Security Breach Indicators*

Initially received July 14, 2021:

- *Privacy Indicators*

Site Visit

Due to COVID-19 public health restrictions, IPC staff did not physically attend the offices of Ontario Health for the purposes of this review. Instead, the IPC reviewed the following location-specific physical access policies and procedures:

- *Government of Ontario IT Standard (GO-ITS) Physical Security Requirements for Data Centres*
- *Ministry of Government and Consumer Services (MGCS) Data Centre Operations Physical Security Access Control Policy and Procedures Guide*
- *Restricted Access at 777 Bay Street Guide*

The IPC met frequently with the Privacy Manager responsible for the review in order to address discrete issues that arose during the review and to discuss the review process and progress generally. Additionally, the following virtual meetings were held between IPC staff and Ontario Health representatives.

June 29, 2021: Consent Management

The IPC requested a meeting with Ontario Health representatives to ask a number of questions about Ontario Health's consent management program with regard to compliance with *PHIPA* and the Manual. The following Ontario Health personnel were in attendance:

- Chief Privacy Officer
- Legal Counsel, Privacy
- Senior Privacy Advisor
- Privacy Manager
- Director, Product Management
- Manager, Product Management

Ontario Health representatives provided the IPC with a PowerPoint presentation that described its consent management program. The presentation was followed by a number of questions and answers exchanged between parties.

September 1, 2021: Physical Access Procedures for 777 Bay Street

The IPC requested a meeting with Ontario Health representatives to receive a description of the physical access procedures for one of its locations where personal health information is handled to fulfil its purposes as the prescribed organization. The following Ontario Health personnel were in attendance:

- Privacy Manager
- Senior Privacy Specialist
- Privacy Specialist
- Project ManagerDirector, Facilities
- Senior Information Security Advisor
- Senior Advisor, IT Risk Management & Compliance
- Coordinator, Corporate Security

Ontario Health representatives provided the IPC with a PowerPoint presentation that described the physical access procedures and safeguards at its 777 Bay Street location. The presentation was followed by a number of questions and answers exchanged between the parties.

Findings of the Review

Privacy Documentation

Privacy Policy in Respect of its Status as the Prescribed Organization

Ontario Health has developed and maintains an overarching *Privacy Policy* to comply with its obligations under applicable privacy laws, including *PHIPA*, the *Freedom of Information and Protection of Privacy Act (FIPPA)* and associated regulations. The *Privacy Policy* refers to policies or procedures that address the following:

- Status under the *Act*
- Privacy and Security Accountability Framework
- Authority to Receive Personal Health Information
- Consent Management
- Minimizing the Personal Health Information Received
- Viewing, Handling or Otherwise Dealing with Personal Health Information
- Providing Personal Health Information to Another Person
- Secure Retention, Transfer and Disposal
- Implementation of Administrative, Technical and Physical Safeguards
- Inquiries, Concerns or Complaints
- Access and Correction
- Transparency of Practices

As set out under paragraph 18 of section 55.3 of *PHIPA*, Ontario Health has in place, and complies with, practices and procedures that have been approved by the Minister of Health for responding to or facilitating a response to a request made by an individual under Part V of the *Act* in respect of the individual's record of personal health information that is accessible by means of the EHR.

Policy and Procedures for Ongoing Review of Privacy Policies, Procedures and Practices

Ontario Health has developed and maintains an overarching *Policy Governance Framework* that ensures a standardized approach for the development, review, approval, implementation, maintenance and repeal of policies and related supporting documents. The requirements and process for the ongoing review of privacy policies, procedures and practices are described in Ontario Health's *Privacy Audit and Compliance Policy*.

Policy on the Transparency of Privacy Policies, Procedures and Practices

Ontario Health has developed and maintains a *Privacy Transparency Policy* that addresses the requirements and process for the transparency of Ontario Health's privacy policies, procedures and practices. The purpose of this policy is to address the information relating to the privacy policies, procedures and practices put in place by Ontario Health that must be made available to the public and to each health information custodian who provides personal health information to Ontario Health, and to identify the means by which such information is made available.

Specifically, the *Privacy Transparency Policy* requires Ontario Health to provide the following on its website:

- Ontario Health's *Privacy Policy*.
- Contact information (including name and/or title, mailing address) to make privacy inquiries, express privacy complaints, request consent directives, and to request access to or correction of personal health information.
- In respect of the EHR:
    - The types of personal health information Ontario Health receives including a description and the persons or organizations from which this personal health information is typically received.
    - A plain language description of the EHR and a general description of the administrative, technical, and physical safeguards in place.
    - Any directives, guidelines and policies that apply to the personal health information that is accessible by means of the EHR.
    - A description of the privacy policies, procedures and practices put in place in respect of personal health information, including:
        - Approved purpose(s) for which employees and other persons acting on behalf of Ontario Health may view, handle or otherwise deal with personal health information; and
        - Ontario Health's required compliance with direction issued pursuant to section 55.9 (3) or 55.10 (1) of *PHIPA*.
- A summary of the results of the threat and risk assessments and privacy impact assessments that are performed for each system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record.
- Documentation related to review and approval by the IPC of Ontario Health's policies, procedures and practices as the prescribed organization.

This information can be accessed at the following web addresses:

- **https://www.ontariohealth.ca/privacy**
- **https://ehealthontario.on.ca/en/our-privacy-commitment**

Policy and Procedures for Receiving Personal Health Information

The requirements and process for receiving personal health information for the purposes of developing and maintaining the EHR are set out in the *EHR Policy for Receiving Personal Health Information*. This policy identifies the process by which personal information is received by Ontario Health, its nature, source and purpose. The policy also addresses the following:

- Review and Approval Process
- Conditions or Restrictions on the Approval
- Secure Retention
- Secure Transfer
- Secure Disposal
- Compliance, Audit and Enforcement
- Notification of Breach

List of Types of Personal Health Information Received

Ontario Health has developed and maintains an up-to-date list of each of the repositories that are accessible by means of the EHR, and a description of the types of personal health information received by Ontario Health that are contained in each repository. This information is maintained in the *EHR Plain Language Description and List of Repositories that are Accessible by the EHR*.

Currently, the EHR consists of the following repositories and registry that contain personal health information received pursuant to *PHIPA* and its regulation:

Repository	Description of PHI	Type of PHI	Source
Acute and Community Clinical Data Repository (acCDR)	Acute clinical information	Patient demographics, emergency department reports, consultation reports, discharge summaries and long-term care placement details including risk assessments and care plans.	Hospitals and home and community care organizations
Diagnostic Imaging-Common Service (DI-CS)	Diagnostic imaging reports and images	Diagnostic imaging reports and images such as X-ray, CT Scan, MRI and ultrasound.	Hospitals, independent health facilities that submitted to the province's three regional Diagnostic Imaging Repositories
Digital Health Drug Repository (DHDR)	Drug and prescription information	Drug and prescription information from publicly-funded drug programs, publicly-funded pharmacy services (e.g. MedsCheck Program, Pharmacy Smoking Cessation Program, vaccine administration) and monitored drugs programs (narcotics and controlled substances) regardless of who the payor is.	Ministry of Health
Primary Care Clinical Data Repository (pcCDR)	Clinical information submitted via certified electronic medical record systems	Patient demographics, medications, allergies, adverse reactions, current health conditions, past medical and surgical history, immunizations, risk factors, vitals and vitals trends.	Primary care providers such as general practitioners or family physicians
Provincial Client Registry (PCR)	Patient demographics and identifiers	Health card numbers, medical record numbers and address information.	Ministry of Health and participating health care organizations
Ontario Laboratories Information System (OLIS)	Laboratory information	Lab test requisitions and results.	Hospitals, community labs and public health labs

Ontario Health provides this information to the public at the following web address:

- **https://ehealthontario.on.ca/en/our-privacy-commitment/plain-language-description-of-the-electronic-health-record**

Policy and Procedures for Descriptions of Types of Personal Health Information Received

The requirements and process for developing and maintaining the descriptions of types of personal health information received by Ontario Health for the purposes of developing and maintaining the EHR are set out in the *EHR Policy for Receiving Personal Health Information*. This policy identifies the process for creating, reviewing, amending, and approving the descriptions of types of personal health information received.

Descriptions of Types of Personal Health Information Received

For each type of personal health information received by Ontario Health for the purpose of developing or maintaining the EHR, Ontario Health has developed and maintains an up-to-date description of:

- The types of personal health information received (e.g. demographic, laboratory, drugs)
- A description of the personal health information (e.g. requisitions, orders, results)
- The source(s) of the personal health information (e.g. Minister, laboratories, hospitals)
- The repository or registry in which the personal health information is contained
- Whether or not the personal health information is received pursuant to the regulation

This information is maintained in the *EHR Plain Language Description and List of Repositories that are Accessible by the EHR*, as well as the *EHR Statement of Information Practices*.

Policy and Procedures for Managing Consent in the Electronic Health Record

An *EHR Consent Directive and Consent Override Policy* has been developed and is maintained. It addresses the following:

- Receiving Requests for Consent Directives
- Implementing and Testing Consent Directives
- Keeping an Electronic Record of and Auditing and Monitoring Consent Directives
- Providing Notice of Consent Directives
- Overrides of Consent Directives
- Keeping an Electronic Record of and Auditing and Monitoring Consent Overrides
- Providing Notice of Consent Overrides
- Reporting Consent Overrides to the IPC
- Responding to Requests for Electronic Records of Consent Directives & Consent Overrides
- Logging
- Compliance, Audit and Enforcement
- Notification of Breach

At the beginning of this review, individuals were able to request the implementation of a consent directive through mail or fax. By the conclusion of the review, individuals are now able to request consent directives by submitting an *EHR Consent Directive Request Form* directly through Ontario Health's website at the following web address:

- **https://ehealthontario.on.ca/en/privacy/managing-access-to-your-ehr**

During the course of the review, the IPC learned that:

a. **Not all health information custodians are currently able to perform consent overrides to all repositories;**
b. **For some repositories a consent override on the basis of a risk of harm is not permitted by the health information custodian that provided the personal health information to the EHR;**
c. **A certain viewer used to access the EHR does not currently have the functionality to distinguish between a consent override made on the basis of a risk of harm to an individual and one made on the basis of a risk of harm to another person or group of persons; and**
d. **Individuals who have implemented consent directives may not have been made aware of the above issues related to consent overrides.**

Consent Overrides

Consent overrides occur when a health information custodian collects personal health information by means of the EHR despite a consent directive that is in place to prevent the health information custodian from accessing that personal health information. *PHIPA* provides the following circumstances where a health information custodian may be permitted to conduct a consent override:

With express consent

Under section 55.7 (1) of *PHIPA*, a health information custodian is permitted to disclose personal health information that is subject to a consent directive by means of the EHR if the health information custodian that is seeking to collect the information obtains the express consent of the individual.

On the basis of a risk of harm

Under section 55.7 (2) of *PHIPA*, a health information custodian is permitted to disclose personal health information that is subject to a consent directive by means of the EHR if the health information custodian seeking to collect the personal health information believes, on reasonable grounds, that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to the individual to whom the information relates and it is not reasonably possible to obtain the individual's consent in a timely manner.

Under section 55.7 (3) of *PHIPA*, a health information custodian may disclose personal health information that is subject to a consent directive by means of the EHR if the health information custodian that is seeking to collect the personal health information believes on reasonable grounds that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom the information relates or to a group of persons.

a. Not all health information custodians are currently able to perform consent overrides to all repositories

Authorized health information custodians access the EHR by direct integration through their electronic medical record (EMR) or hospital information system (HIS) or through Ontario Health-operated provincial viewers. Some health information custodians are unable to conduct a

consent override when using their own EMR or HIS to integrate with the EHR. However, consent overrides can be conducted using a provincial viewer. The only exception to this is with respect to the DI-CS repository; a consent override cannot currently be conducted for this repository using a provincial viewer. This means that nearly all health information custodians are unable to complete a consent override to access the DI-CS repository.

Ontario Health is in the process of determining how to address this issue and has indicated that it may do so in one of three possible ways:

- Support the vendors of the health information systems that do not currently offer consent override functionality to use the Provincial Consent Override Interface (PCOI), an interface developed by Ontario Health;
- Upgrade the existing Ontario Health-operated provincial viewer to include this functionality when accessing the DI-CS; or
- Replace the existing Ontario Health-operated provincial viewer with a provincial viewer that includes this functionality.

Recommendation:

Provide the IPC with a detailed plan, complete with timelines, that ensures the timely implementation of a mechanism to enable all health information custodians to perform a consent override pursuant to subsections 55.7 (1)-(3) of *PHIPA* when attempting to access personal health information within the DI-CS repository.

b. In some repositories a consent override on the basis of a risk of harm is not permitted

It is currently not possible for health information custodians to perform a consent override when attempting to access personal health information within OLIS and DHDR on the basis of a risk of harm to either the individual or to another person or group of persons (ss. 55.7 (2) and (3) of *PHIPA*). Ontario Health has indicated that these repositories have given Ontario Health instructions to only permit consent overrides on the basis of express consent (s. 55.7 (1)).

Recommendation:

Continue to consult with the IPC to address the circumstances where a consent override is not currently possible pursuant to subsection 55.7 (2) or (3) of *PHIPA*, including when attempting to access personal health information within the Ontario Laboratory Information System (OLIS) and the Digital Health Drug Repository (DHDR).

c. A certain viewer used to access the EHR does not currently have the functionality to distinguish between a consent override made on the basis of a risk of harm to an individual and an override made on the basis of a risk of harm to another person or group of persons

The ConnectingOntario viewer does not enable health information custodians to distinguish whether they are performing a consent override based on the grounds set out in subsection 55.7 (2) or (3).

The regulation under *PHIPA* requires notice to be provided to health information custodians and individuals regarding consent overrides and each of these notices is required to identify the reason for the consent override (s. 18.6 (d) and 18.7 (d) of O.Reg 329/04). Additionally, subsection 55.7 (7) (b) of *PHIPA* states that the health information custodian that collected personal health information through a consent override for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom the information relates or to a group of persons, must give written notice to the IPC. To comply with these sections of *PHIPA* and its regulation, the clinical viewer must distinguish the grounds upon which the override is performed.

Ontario Health is in the process of conducting an options analysis to assess whether separating consent overrides under subsections 55.7 (2) and 55.7 (3) of *PHIPA* will be addressed by way of an update to the ConnectingOntario clinical viewer or built into a new consolidated clinical viewer that may be developed. Where external dependencies exist, Ontario Health is working with its vendors to understand costing and resource requirements.

Recommendation:

Provide the IPC with a detailed plan, complete with timelines, for implementing expanded functionality within the ConnectingOntario clinical viewer to ensure that health information custodians accessing the electronic health record through this method are able to distinguish whether a consent override is being conducted for the purposes of subsection 55.7 (2) or (3) of *PHIPA*.

d. Individuals who have implemented consent directives have not been made aware of the above issues related to consent overrides

Individuals who have requested the implementation of a consent directive may not have been made aware that there are circumstances where health information custodians may not be able to perform a consent override. Individuals may reasonably have believed that their consent directives could be overridden with their express consent or in circumstances where it is necessary to eliminate or reduce significant risk of serious bodily harm. If individuals have not been made aware of the fact that, in some instances, health information custodians may not be able to override their consent directives, including where there is a significant risk of serious bodily harm to the individual, individuals may not be able to make a fully informed decision regarding the implementation of a consent directive.

Recommendation:

Until all health information custodians have the functionality to perform consent overrides (for the purposes of section 55.7 of *PHIPA*) for all repositories within the electronic health record, take reasonable steps to ensure that individuals who request a consent directive and have previously requested a consent directive are provided with notice that consent overrides may not be possible in the circumstances described above so that they are aware of the risks. It is further recommended that Ontario Health continue to consult with the IPC regarding the notice before implementation.

Log of Notices of Consent Directives

When a health information custodian attempts to view an individual's personal health information that is subject to a consent directive, an electronic alert (notice of consent directive) is presented to the user in the clinical user interface to notify the health information custodian that a consent directive is in place blocking access to the personal health information.

Ontario Health does not maintain a log of each instance an end user is notified of the existence of a consent directive. However, the IPC is satisfied that Ontario Health has implemented other measures to ensure that notices are being displayed correctly.

Every consent directive is tested after it is implemented and Ontario Health conducts functional testing and auditing of its consent management products. Controls are in place to ensure that the electronic alerts continue to function properly and without disruption ("service health checks").

Service health checks are a method for ensuring the electronic alert function notifies the user each time they attempt to view an individual's information that is subject to a consent directive block. Service health checks mimic an end user's interaction with the EHR to ensure that the directive is displaying as it is expected to. Service health checks are supported by technical staff and procedures to initiate corrective actions in the event of a failed service health check.

Log of Notices of Consent Overrides

Appendix A of the *EHR Consent Directive and Consent Override Policy* describes the maintenance of a log of notices of consent overrides that meets the requirements of the Manual.

Log of Reports of Consent Overrides to the IPC

Appendix A of the *EHR Consent Directive and Consent Override Policy* describes the maintenance of a log of annual reports that are required to be provided to the IPC that meets the requirements of the Manual.

Log of Requests for Electronic Records from Health Information Custodians

Appendix A of the *EHR Consent Directive and Consent Override Policy* describes the maintenance of a log of requests for electronic records from health information custodians that meets the requirements of the Manual.

Log of Requests for Electronic Records from the IPC

Appendix A of the *EHR Consent Directive and Consent Override Policy* describes the maintenance of a log of requests for electronic records from the IPC that meets the requirements of the Manual.

Log of Audits of the Electronic Records of Consent Directives and Consent Overrides

Appendix A of the *EHR Consent Directive and Consent Override Policy* describes the maintenance of a log of audits of the electronic records of consent directives and consent overrides that meets the requirements of the Manual.

Policy and Procedures for Viewing, Handling or Otherwise Dealing with Personal Health Information by Employees and Other Persons Acting on Behalf of the Prescribed Organization

A *Privacy Use and Disclosure Policy* has been developed and is maintained by Ontario Health to identify the purposes and the circumstances for which personal health information received for the purpose of developing or maintaining EHR may be viewed, handled or otherwise dealt with by employees and other persons acting on behalf of Ontario Health.

The *Privacy Use and Disclosure Policy* addresses the following:

- Levels of Access
- Review and Approval Process
- Conditions or Restrictions on Approval
- Notification and Termination of Permission to View, Handle or Otherwise Deal with Personal Health Information
- Secure Retention
- Secure Disposal
- Tracking Approval to View, Handle or Otherwise Deal with Personal Health Information
- Compliance, Audit and Enforcement
- Notification of Breach

Log of Employees and Other Persons Acting on Behalf of the Prescribed Organization Granted Permission to View, Handle or Otherwise Deal with Personal Health Information

Appendix C of the *Privacy Use and Disclosure Policy* describes the maintenance of a log of employees and other persons acting on behalf of Ontario Health granted permission to view, handle or otherwise deal with personal health information that meets the requirements of the Manual.

Policy and Procedures for the Provision of Personal Health Information Pursuant to sections 55.9 (3) or 55.10 (1)

Ontario Health has developed and maintains a *Privacy Use and Disclosure Policy* that addresses the following matters in receiving a direction issued pursuant to subsections 55.9 (3) or 55.10 (1) of *PHIPA*:

- Receiving the direction
- Implementing the direction
- Secure transfer
- Logging
- Compliance, auditing and enforcement
- Notification of breach

Log of Directions

Appendix A of the *Privacy Use and Disclosure Policy* describes the maintenance of a log of directions issued pursuant to subsections 55.9 (3) or 55.10 (1) of *PHIPA* that meets the requirements of the Manual.

Policy and Procedures for Responding to Requests for Access and Correction of Records of Personal Health Information

Subsections 51 (5) and (6) of *PHIPA*, when in force, will apply Part V of the *Act*, related to access and correction of personal health information, to the prescribed organization. As these sections are not currently in force, Ontario Health does not currently have the authority to respond to requests for access or correction of records of personal health information within the EHR. However, individuals continue to be able to make these requests through the health information custodians with custody or control of the information.

As set out above, Ontario Health must have in place and comply with practices and procedures that have been approved by the Minister of Health for responding to or facilitating a response to a request made by an individual under Part V of the *Act* in respect of the individual's record of personal health information that is accessible by the EHR.

Ontario Health has policies and procedures in place to address its role in responding to or facilitating a response to a request made by an individual under Part V of *PHIPA* in respect of personal health information available through the EHR pursuant to its obligation in paragraph 18 of section 55.3. The *EHR Request for Access to Personal Health Information Policy and Procedure* and the *EHR Request for Correction to Personal Health Information Policy and Procedure* address the following:

- Receiving and reviewing requests
- Responding to requests
- Facilitating a response to requests
- Notice to the public
- Tracking requests
- Compliance, audit and enforcement
- Breach notification

Log of Access and Correction Requests

Appendix A of the *EHR Request for Access to Personal Health Information Policy and Procedure* and Appendix A of the *EHR Request for Correction to Personal Health Information Policy and Procedure* describe the maintenance of logs of access and correction requests that meet the requirements of the Manual.

Policy and Procedures for Executing Agreements with Third Party Service Providers

Ontario Health's *Privacy Use and Disclosure Policy* addresses the following matters relating to executing agreements with third party service providers:

- Limitation on provision and the viewing, handling and otherwise dealing with personal health information
- Secure transfer
- Prohibition on disclosure of personal health information by the third party service provider
- Tracking agreements
- Compliance, audit and enforcement
- Notification of breach

Template Agreement for All Third Party Service Providers

Ontario Health has established a template written agreement, *Schedule for Privacy, Security and Confidentiality for Third Party Service Provider Agreements*, that is used as the basis for entering into

written agreements with third party service providers contracted or otherwise engaged to provide services to Ontario Health who will be permitted to view, handle or otherwise deal with personal health information provided to Ontario Health for the purpose of developing or maintaining the EHR.

The *Schedule for Privacy, Security and Confidentiality for Third Party Service Provider Agreements* addresses the following:

- General provisions
- Obligations with respect to viewing, handling or otherwise dealing with personal health information
- Prohibition on disclosure
- Secure transfer
- Secure retention
- Secure return or disposal following termination of the agreement
- Secure disposal as a contracted service
- Implementation of safeguards
- Training employees or other persons acting on behalf of the third party service provider
- Subcontracting of the services
- Notification
- Consequences of breach and monitoring compliance

Log of Agreements with Third Party Service Providers

Appendix B of the *Privacy Use and Disclosure Policy* describes the maintenance of a log of agreements with third party service providers that meets the requirements of the Manual.

Privacy Impact Assessment Policy and Procedures

A *Privacy Impact Assessment (PIA) Standard* has been developed to identify the circumstances in which PIAs are required to be conducted and to address the process and criteria used to identify privacy risks arising from new programs or changes within the organization (e.g. to a program, technology or policy) and recommend strategies and an action plan to address the privacy risk. The *PIA Standard* addresses the following:

- Circumstances in which a PIA must be conducted
- Contents of PIA
- PIA recommendations
- Log of PIAs
- Compliance, audit and enforcement
- Notification of breach

Log of Privacy Impact Assessments

Appendix B of the *PIA Standard* describes the maintenance of a log of PIAs that meets the requirements of the Manual.

Policy and Procedures in Respect of Privacy Audits

A *Privacy Audit and Compliance Policy* has been developed and is maintained by Ontario Health to set out the types of privacy audits that are required to be conducted in respect of all personal health information and personal information received by Ontario Health and to identify the process for conducting privacy audits.

The *Privacy Audit and Compliance Policy* addresses the following:

- Types of audits to be conducted
- Process for conducting privacy audits
- Tracking privacy audits
- Compliance, audit and enforcement
- Notification of breach

Log of Privacy Audits

Appendix B of the *Privacy Audit and Compliance Policy* describes the maintenance of a log of privacy audits that meets the requirements of the Manual.

Policy and Procedures for Privacy Breach Management

Ontario Health has developed and maintains a *Privacy Incident Management Policy and Procedure* and an *EHR Privacy Incident Management Policy and Procedure* to address the identification, reporting, containment, notification, investigation and remediation of privacy incidents in respect of the personal health information it receives, including personal health information it receives for the purpose of developing or maintaining the EHR.

The *Privacy Incident Management Policy and Procedure* includes requirements and processes to manage privacy incidents caused by Ontario Health or an unauthorized party related to any personal health information or personal information received by Ontario Health, while the *EHR Privacy Incident Management Policy and Procedure* addresses processes that are specific to managing privacy incidents related to the EHR.

Together, these documents address the following:

- Identification of privacy breaches
- Privacy breaches caused by one or more health information custodians
- Privacy breaches caused by the prescribed organization or an unauthorized person
- Communication of findings of investigation and recommendations
- Tracking privacy breaches
- Relationship to policy and procedures for information security breach management
- Compliance, audit and enforcement

Log of Privacy Breaches

Appendix C of the *Privacy Incident Management Policy and Procedure* describes the maintenance of a log of privacy breaches that meets the requirements of the Manual.

Policy and Procedures for Privacy Complaints

Ontario Health has developed and maintains a *Privacy Complaints and Inquiries Policy* and an *EHR Inquiries and Complaints Policy and Procedure* to address the process to be followed in receiving, documenting, tracking, investigating, remediating and responding to privacy complaints and privacy inquiries in respect of the personal health information it receives, including personal health information accessible by means of the EHR.

The *Privacy Complaints and Inquiries Policy* includes the requirements and processes to manage privacy complaints and inquiries related to Ontario Health, while the *EHR Inquiries and Complaints Policy and Procedure* addresses the requirements and the processes that are specific to managing complaints and inquiries related to the EHR.

Together, these documents address the following:

- Process for receiving complaints
- Complaints related to one or more health information custodians
- Complaints related to the prescribed organization or an unauthorized person
- Tracking privacy complaints
- Relationship to policy and procedures for privacy breach management
- Compliance, audit and enforcement
- Notification of breach

Log of Privacy Complaints

Appendix A of the *Privacy Complaints and Inquiries Policy* and Appendix A of the *EHR Privacy inquiries and Complaints Policy and Procedure* describe the maintenance of logs of privacy complaints that meet the requirements of the Manual.

Policy and Procedures for Privacy Inquiries

Ontario Health has developed and maintains a *Privacy Complaints and Inquiries Policy* and an *EHR Inquiries and Complaints Policy and Procedure* to address the process to be followed in receiving, documenting, tracking and responding to privacy inquiries in respect of personal health information that is accessible by means of the EHR.

The *Privacy Complaints and Inquiries Policy* includes the requirements and processes to manage privacy complaints and inquiries related to Ontario Health, while the *EHR Inquiries and Complaints Policy and Procedure* addresses the requirements and the processes that are specific to managing complaints and inquiries related to the EHR.

Together, these documents address the following:

- Inquiries related to one or more health information custodians
- Inquiries related to Ontario Health or an unauthorized person
- Compliance, audit and enforcement
- Notification of breach

Security Documentation

Information Security Policy

An overarching *Information Security Policy* has been developed and is maintained by Ontario Health that requires steps be taken that are reasonable in the circumstances to ensure that personal health information accessible by means of the EHR is not collected without authority, and is protected against theft, loss and unauthorized use or disclosure, and that records of personal health information accessible by means of the EHR are protected against unauthorized copying, modification or disposal.

The *Information Security Policy* addresses the following:

- Threat and risk assessment
- Information security program
- Information security infrastructure
- Continuous assessment and verification of the security program

- Compliance, audit and enforcement
- Notification of breach

Policy and Procedures for Ongoing Review of Security Policies, Procedures and Practices

Ontario Health has developed and maintains a *Policy Governance Framework* to provide a framework for policy development and governance within the organization. The *Policy Governance Framework* ensures a standardized approach for the development, review, approval, implementation, maintenance and repeal of policies and related supporting documents.

The requirements and process for the ongoing review of security policies, procedures and practice is described in the *Information Security Program Governance*. *The Information Security Program Governance* further addresses the ongoing review of the security policies, procedures and practices put in place by Ontario Health.

Policy and Procedures for Ensuring Physical Security of Personal Health Information

Ontario Health has developed and maintains four primary documents to address the physical safeguards put in place to protect the personal health information accessible by means of the EHR. The requirements and process for ensuring physical security of personal health information are described in the *Physical and Environmental Security Standard*. The *Physical Access Policy* sets out the requirements for controlling, monitoring and removing access to the physical environments operated by Ontario Health. The *Access Card Procedure* describes the steps for the issuance, use, revocation and accountability of access cards to Ontario Health premises. The *Visitor Access Procedure* describes the policy, procedure and practices with respect to access by visitors.

Together, these documents address the following:

- Policy, procedures and practices with respect to access by employees and other persons acting on behalf of Ontario Health
    - Theft, loss and misplacement of identification cards, access cards and keys
    - Termination or cessation of the employment, contractual or other relationship
    - Notification when access is no longer required
    - Audits of employees or other persons acting on behalf of the prescribed organization with access to the premises
    - Tracking and retention of documentation related to access to the premises
- Policy, procedures and practices with respect to access by visitors
- Compliance, audit and enforcement
- Notification of breach

Log of Employees or Other Persons Acting on behalf of the Prescribed Organization with Access to the Premises of the Prescribed Organization

The *Access Card Procedure* and the *Visitor Access Procedure* describe the maintenance of a log of employees or other persons acting on behalf of Ontario Health with access to the premises of the organization that meets the requirements of the Manual.

Policy and Procedures for Secure Retention of Records of Personal Health Information

Ontario Health has developed and maintains three primary documents to address the secure retention of records of personal health information accessible by means of the EHR either in paper or electronic format.

The *Personal Health Information Handling Standard* establishes a framework of approved methods and safeguards for ensuring the secure handling of personal health information so that Ontario Health continues to meet its obligations under *PHIPA* and the Manual. The *Information Classification and Handling Standard* defines risk-based classification schemes for information within Ontario Health. The *Information Classification and Handling Guideline* provides guidelines for the implementation of the *Information Classification Handling Standard* including instructions and examples on how to classify Ontario Health's information assets and protect information assets during their lifecycles (e.g. creation, access, modification, disposal or destruction).

Together, these documents address the following:

- Retention period
- Secure retention
- Third party service providers
- Compliance, audit and enforcement
- Notification of breach

Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices

Ontario Health has developed and maintains a *Mobile Security Standard* which describes security requirements for the use of mobile devices at Ontario Health. The *Mobile Security Standard* addresses the following:

- Where personal health information is permitted to be retained on a mobile device
  - Approval process
  - Conditions or restrictions on the retention of personal health information on a mobile device
- Where personal health information is not permitted to be retained on a mobile device
  - Approval process
  - Conditions or restrictions on remote access to personal health information
- Compliance, audit and enforcement
- Notification of breach

Policy and Procedures for Secure Transfer of Records of Personal Health Information

Ontario Health has developed and maintains a *Secure Transfer of Sensitive Information Standard* that addresses the secure transfer of records of personal health information received for the purpose of developing or maintaining the EHR in paper and electronic format. The purpose of this standard is to ensure the protection of personal health information in accordance with *PHIPA* when transferred, processed, and received. Personal health information is classified as high sensitivity in accordance with the *Information Classification and Handling Standard*.

Together, these documents address the following:

- Approved methods of secure transfer
- Process of secure transfer
- Administrative, technical and physical safeguards to ensure secure transfer
- Compliance, audit and enforcement
- Notification of breach

Policy and Procedures for Secure Disposal of Records of Personal Health Information

Ontario Health has developed and maintains two primary documents to address the secure disposal of records of personal health information received for the purpose of developing or maintaining the EHR in both paper and electronic format in order to ensure that reconstruction of these records is not reasonably foreseeable in the circumstances.

The *Media Destruction, Sanitization and Disposal Standard* describes the requirements for the destruction, sanitization, and disposal of digital media. The *Hard Copy Personal Health Information/Personal Information and Media Destruction Procedure* describes the requirements for the secure destruction of hard-copy records containing personal health information or personal information.

Together, these documents address the following:

- Methods of secure disposal
- Secure retention pending disposal
- Process of secure disposal
- Compliance, audit and enforcement
- Notification of breach

The IPC is of the view that maintaining the *Hard Copy Personal Health Information/Personal Information and Media Destruction Procedure* and *Media Destruction, Sanitization and Disposal Standard* as two standalone documents provides opportunity for gaps and overlaps that will require close monitoring as these policies are maintained over time by separate departments within the organization. The IPC accepts Ontario Health's interest to maintain these as two separate documents, but has requested further clarification of language. Ontario Health will continue to consult with our office at the conclusion of the review to address this concern.

Policy and Procedures Relating to Passwords

An *Access Control Standard* has been developed and is maintained by Ontario Health to ensure Ontario Health controls access to its assets. The *Access Control Standard* describes requirements for employees and other persons acting on behalf of Ontario Health regarding logical access to Ontario Health assets and addresses the requirements in the Manual relating to passwords.

Policy and Procedures in Respect of Privacy Notices

A *Privacy Notices Policy and Procedure* has been developed and is maintained by Ontario Health that outlines the process implemented by Ontario Health relating to privacy notices that are required to be displayed on all information systems and technologies maintained by Ontario Heath involving personal health information.

Employees and other persons acting on behalf of Ontario Health access personal health information through information systems that are developed and provided by third parties. While there are technological limitations associated with modifying these vendor systems to display customized privacy notices, Ontario Health has implemented a process where a privacy notice, customized by and for Ontario Health's purposes, is displayed at the first point of entry to Ontario Health's EHR information systems. For example, each time a user logs on to an Ontario Health laptop, the user is presented with the privacy notice, where they are required to review, acknowledge, and agree to the terms of the privacy notice.

Policy and Procedures for Acceptable Use Agreements with Employees and Other Persons Acting On Behalf of the Prescribed Organization

Ontario Health has implemented an *Information Security Acceptable Use Policy* that requires employees and other persons acting on behalf of Ontario Health to acknowledge and agree to comply with its *Acceptable Use Agreement*. The *Information Security Acceptable Use Policy* addresses the following:

- Timing of acceptable use agreements
- Process for ensuring employees and other persons acting on behalf of Ontario Health acknowledge and agree to comply with the acceptable use agreement
- Tracking acceptable use agreements
- Compliance, audit and enforcement
- Notification of breach

Template Acceptable Use Agreement with Employees and Other Persons Acting on behalf of the Prescribed Organization

Ontario Health has developed and maintains an *Acceptable Use Agreement for Ontario Health Employees and Other Agents Template* that must be acknowledged and agreed to by each employee or other person acting on behalf of Ontario Health in accordance with Ontario Health's *Information Security Acceptable Use Policy*.

The *Acceptable Use Agreement for Ontario Health Employees and Other Agents Template* addresses the following:

- Obligations with respect to viewing, handling and otherwise dealing with personal health information
- Administrative, technical and physical safeguards
- Consequences of breach and monitoring compliance
- Required acknowledgement and agreements

Log of Acceptable Use Agreements

Appendix A of the *Information Security Acceptable Use Policy* describes the maintenance of a log of acceptable use agreements that meets the requirements of the Manual.

Policy and Procedures for End User Agreements

Ontario Health has developed and maintains an *EHR Policy and Procedures for Agreements with Health Information Custodians and Coroners* to address the process to be followed to ensure that health information custodians, coroners and their agents (end users) who provide personal health information to the EHR or collect personal health information by means of the EHR are aware of, and comply with, certain privacy and security obligations.

The *EHR Policy and Procedures for Agreements with Health Information Custodians and Coroners* requires Ontario Health to ensure that health information custodians and coroners under whose authority personal health information is provided to the EHR or collected by means of the EHR acknowledge and agree to comply with the relevant Ontario Health contributor or access services agreement that addresses the matters set out in the Manual. This also requires health information custodians and coroners to require their end users to comply with the obligations. These requirements are incorporated into the minimum content requirements set out in Appendix A to the *EHR Policy and Procedures for Agreements with Health Information Custodians and Coroners*:

- Obligations with respect to collection, use and disclosure of personal health information
- Administrative, technical and physical safeguards
- Consequences of breach and monitoring compliance
- Required acknowledgements and agreements

The Manual requires that the prescribed organization develop and implement a policy and procedures requiring each end user who provides personal health information to, or collects personal health information by means of, the EHR to acknowledge and agree to comply with an end user agreement. However, Ontario Health does not currently have in place agreements directly with each end user.

Instead, Ontario Health executes relevant contributor or access services agreements with all health information custodians and coroners under whose authority personal health information is provided to the EHR or collected by means of the EHR. Ontario Health relies on the contributor or access services agreement between Ontario Health and the health information custodian or coroner to ensure the compliance of each of its respective agents (end users) with the terms of the agreement.

These agreements address the following matters set out in the Manual with respect to end user agreements (as listed in Appendix A to the *EHR Policy and Procedures for Agreements with Health Information Custodians and Coroners*):

- Timing of agreements
- Process for ensuring health information custodians agree to comply with the agreement
- Tracking agreements
- Compliance, audit and enforcement
- Notification of breach

Given the high volume of end users (over 7,300 organizations and over 225,000 eligible and authorized users accessing EHR data), Ontario Health has indicated that it would be onerous to administer agreements directly with each of the end users of the EHR. The IPC accepts that using contractual measures with health information custodians and coroners may be a reasonable alternative to having agreements in place with each end user. However, currently, the agreements with health information custodians and coroners do not include provisions that require the health information custodians or coroners: 1) to ensure that their agents regularly acknowledge and agree to the terms set out in the agreement with Ontario Health (at least annually), and 2) to maintain a log that tracks the administration and acknowledgement of these agreements, as required by the Manual.

In the IPC's view, health information custodians and coroners should ensure their agents acknowledge and agree to comply with the privacy and security obligations set out in the agreement between Ontario Health and health information custodians and coroners on a regular basis. Furthermore, health information custodians and coroners should maintain a log of end users who have acknowledged and agreed to these obligations.

The IPC hereby requests Ontario Health to continue to consult with our office after the end of the review period as they work toward addressing the below recommendation.

Recommendation:

In consultation with the IPC:

- Develop a proposal and accompanying plan that provides assurance that all health information custodians and coroners have implemented an acceptable method for receiving an acknowledgement and agreement from end users to comply with the privacy and security obligations set out in the agreements between Ontario Health and health information custodians and coroners on a regular basis (at least annually).
- Ensure that the proposal and plan, described above, provides assurance that health information custodians and coroners are keeping track of these acknowledgements in a manner that can be easily audited by health information custodians, coroners and Ontario Health.

Template End User Agreements

The section above, **Policy and Procedures for End User Agreements**, discusses Ontario Health's compliance with this section of the Manual.

Log of End User Agreements

Ontario Health maintains a log of all Ontario Health contributor and access services agreements acknowledged and agreed to by health information custodians and coroners under whose authority personal health information is provided to or collected by means of the EHR. As discussed above, Ontario Health does not maintain a log of end user agreements; however, they do maintain a log of agreements with health information custodians and coroners.

The log of contributor and access services agreements sets out, at a minimum:

- The name of each health information custodian or coroner under whose authority personal health information will be provided to or collected by means of the EHR; and
- The dates that the relevant Ontario Health contributor or access services agreement was acknowledged and agreed to.

These requirements are incorporated into the log requirements set out in Appendix B to the *EHR Policy and Procedures for Agreements with Health Information Custodians and Coroners*.

As noted above, the current contractual agreements between Ontario Health and the health information custodian or coroner do not require that a log be kept of each end user who acknowledges and agrees to these same terms, as set out in the Manual. To address this, see the recommendation set out above.

Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs

Ontario Health has developed and maintains an *Information Security Operations Standard*, which, along with the *EHR Privacy Auditing and Monitoring Policy*, addresses the creation, maintenance and ongoing review of system control and audit logs involving personal health information that is accessible by means of the EHR.

The *Information Security Operations Standard* addresses the following:

- Logging functionality
- Content of logs
- Retention of logs
- Auditing and monitoring
- Responding to requests for electronic records
- Logging
- Compliance, audit and enforcement
- Notification of breach

Log of Requests for Electronic Records from Health Information Custodians

Appendix B of the *EHR Privacy Auditing and Monitoring Policy* describes the maintenance of a log of requests for electronic records from health information custodians that meets the requirements of the Manual.

Log of Requests for Electronic Records from the IPC

Appendix A of the *EHR Privacy Auditing and Monitoring Policy* describes the maintenance of a log of requests for electronic records from the IPC that meets the requirements of the Manual.

Policy and Procedures for Patch Management

Ontario Health has developed and maintains an *Information Security Operations Standard* that addresses the requirements for patch management of all information systems, technologies, equipment, resources, applications and programs used to create and maintain the EHR. The *Information Security Operations Standard* addresses the following:

- Patch monitoring
- Patch analysis
- Patch implementation
- Compliance, audit and enforcement
- Notification of breach

Policy and Procedures for Change Management

Ontario Health's *Information Security Operations Standard* addresses the requirements for reviewing and determining whether to approve a change to Ontario Health's operational environment in creating or maintaining the EHR. This includes:

- Roles, responsibilities, and processes to be followed in reviewing and approving changes to operational environments
- The criteria considered when approving or denying a request for a change to the operational environment
- The decision-making process and documentation required when approving or denying the request for a change to the operational environment
- The process for implementation of changes to the operational environment
- The policy and procedure for testing changes to the operational environment
- The documentation required to be maintained of changes that have been implemented

Policy and Procedures for Back-Up and Recovery of Records of Personal Health Information

Ontario Health's *Information Security Operations Standard* addresses the requirements for a policy and procedures for the back-up and recovery of records of personal health information received by Ontario Health for the purpose of developing or maintaining the EHR.

The *Information Security Operations Standard* addresses the following:

- Testing the procedure for back-up and recovery
- Third party service providers
- Availability of backed-up records
- Compliance, audit and enforcement
- Notification of breach

Policy and Procedures on the Acceptable Use of Technology

Ontario Health has developed and maintains an *Information Security Acceptable Use Policy* that outlines the acceptable use of information systems, technologies, equipment, resources, applications and programs used for the purpose of developing or maintaining the EHR regardless of whether they are owned, leased or operated by Ontario Health.

The *Information Security Acceptable Use Policy* addresses the following:

- The uses that are prohibited without exception, the uses that are permitted without exception and the uses that are permitted only with prior approval
- The roles, responsibilities, requirements, process, and documentation that must be completed in regard to uses of technology that are permitted only with prior approval
- Compliance, Audit and Enforcement
- Notification of Breach

Threat and Risk Assessment Policy and Procedures

Ontario Health has developed and maintains an *Information Security Risk Management Standard* that identifies the circumstances in which threat and risk assessments (TRA) are required to be conducted, including:

- Circumstances in which TRAs must be conducted
- TRA methodology
- Process for addressing TRA recommendations
- Log of TRAs
- Compliance, audit and enforcement
- Notification of breach

Log of Threat and Risk Assessments

The *Information Security Risk Management Standard* describes the maintenance of a log of TRAs that meets the requirements of the Manual.

Policy and Procedures in Respect of Security Audits

Ontario Health has developed and maintains an *Information Security Risk Management Standard* that sets out the types of security audits that are required to be conducted.

Log of Security Audits

The *Information Security Risk Management Standard* describes the maintenance of a log of security audits that meets the requirements of the Manual.

Policy and Procedures for Information Security Breach Management

Ontario Health has developed and maintains two primary documents to address the identification, reporting, containment, notification, investigation and remediation of information security breaches.

Together, the *Information Security Incident Management Standard* and the *External Information Security Incident Management Standard* address the following:

- Identification of information security breaches
- Information security breaches caused by one or more health information custodians
- Information security breaches caused by Ontario Health or an unauthorized person
    - Determination of whether a security breach occurred
    - Containment
    - Notification
    - Investigation and recommendations
    - Communication of findings of investigation and recommendations
    - Tracking information security breaches
- Relationship to policy and procedures for privacy breach management
- Compliance, audit and enforcement
- Notification of breach

Log of Information Security Breaches

The *Information Security Incident Management Standard* and the *External Information Security Incident Management Standard* describe the maintenance of a log of security breaches that meets the requirements of the Manual.

Human Resources Documentation

Policy and Procedures for Privacy Training and Awareness

A *Privacy and Security Training and Awareness Policy and Procedure* has been developed and is maintained by Ontario Health that requires employees and other persons acting on behalf of Ontario Health to attend initial privacy training as well as ongoing privacy training. This policy has been developed in relation to all personal health information and personal information collected or received by Ontario Health, including personal health information received by Ontario Health for the purposes of developing and maintaining the EHR.

The *Privacy and Security Training and Awareness Policy and Procedure* addresses the following:

- Timing and method of initial and ongoing privacy training
- Process for preparing the content and delivering privacy training
- Content of initial privacy training
- Content of ongoing privacy training
- Tracking, auditing and monitoring privacy training
- Other mechanisms to foster a privacy culture
- Compliance, audit and enforcement
- Notification of breach

Log of Attendance at Initial and Ongoing Privacy Training

The *Privacy and Security Training and Awareness Policy and Procedure* describes the maintenance of a log of attendance at initial and ongoing privacy training that meets the requirements of the Manual.

Policy and Procedures for Security Training and Awareness

The *Privacy and Security Training and Awareness Policy and Procedure* addresses the following:

- Timing and method of initial and ongoing security training
- Process for preparing the content and delivering security training
- Content of initial security training
- Content of ongoing security training
- Tracking, auditing and monitoring security training
- Other mechanisms to raise security awareness
- Compliance, audit and enforcement
- Notification of breach

Log of Attendance at Initial and Ongoing Security Training

The *Privacy and Security Training and Awareness Policy and Procedure* describes the maintenance of a log of attendance at initial and ongoing security training that meets the requirements of the Manual.

Policy and Procedures for the Execution of Confidentiality Agreements by Employees and Other Persons Acting on behalf of the Prescribed Organization

A *Confidentiality Agreements Policy* has been developed and is maintained by Ontario Health that requires employees and other persons acting on behalf of Ontario Health to execute a confidentiality agreement that contains the language from Ontario Health's *Confidentiality Agreement Template*.

The *Confidentiality Agreement Policy* addresses the following:

- Timing of confidentiality agreements
- Process for executing confidentiality agreements
- Tracking execution of confidentiality agreements
- Compliance, audit and enforcement
- Notification of breach

Template Confidentiality Agreement with Employees and Other Persons Acting on behalf of the Prescribed Organization

A *Confidentiality Agreement Template* developed and maintained by Ontario Health must be executed by each employee or other person acting on behalf of Ontario Health in accordance with the *Confidentiality Agreement Policy*. The *Confidentiality Agreement Template* addresses the following:

- General provisions
- Required compliance
- Obligations with respect to viewing, handling or otherwise dealing with personal health information
- Obligations with respect to de-identified and aggregate information
- Termination of the contractual, employment or other relationship
- Notification
- Consequences of breach and monitoring compliance

Log of Executed Confidentiality Agreements with Employees and Other Persons Acting on behalf of the Prescribed Organization

The *Confidentiality Agreement Policy* describes the maintenance of a log of executed confidentiality agreements with employees and other persons acting on behalf of Ontario Health that meets the requirements of the Manual.

Job Description for the Position(s) Delegated Day–to–Day Authority to Manage the Privacy Program

The *Chief Privacy Officer (CPO) Job Description* identifies the *Chief Privacy Officer* as being delegated day-to-day authority to manage the privacy program on behalf of Ontario Health. The *CPO* reports to the *Executive Lead of the Legal, Privacy and Risk Portfolio*. The *CPO* job description identifies the responsibilities and obligations of this position in respect of the privacy program.

Job Description for the Position(s) Delegated Day–to–Day Authority to Manage the Security Program

Ontario Health has identified two roles within the organization that have been delegated day-to-day authority to manage the security program on behalf of Ontario Health.

The *Vice President (VP), Innovations for Connected Health* reports to the *Digital Excellence in Health Executive*, who reports to the *Chief Executive Officer (CEO)*. The *VP, Innovations for Connected Health* is accountable for developing, implementing, and monitoring a strategic, comprehensive information security program to ensure appropriate levels of confidentiality, integrity, availability, safety, privacy, and recovery of information assets owned, controlled, and processed by Ontario Health.

The *Director, Enterprise Information Security Office* reports directly to the *VP, Innovations for Connected Health* and supports both the VP and the *Digital Excellence Portfolio Executive* in raising awareness to the CEO on cyber security manners. The *Director, Enterprise Information Security Office* is responsible for leading the development and maintenance of the *Information Security Governance Framework*, together with the associated policies, standards and processes. They are also responsible for consulting and advisory services provided to projects and business/technology groups (which includes but is not limited to threat risk assessments and risk-based information security solutions) and for monitoring and ensuring compliance with the *Information Security Governance Framework* across Ontario Health.

Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship

Ontario Health has developed and maintains a *Termination of Employment Policy* to clarify the requirements and processes that must be followed when an employee or other person acting on behalf of Ontario Health leaves Ontario Health either voluntarily or involuntarily.

The *Termination of Employment Policy* addresses the following:

- Secure return of all property
- Terminating access to premises and operational environments
- Compliance, audit and enforcement
- Notification of breach

Policy and Procedures for Discipline and Corrective Action

Ontario Health has developed a *Progressive Discipline Policy* to set out the requirements and associated procedures for discipline and corrective action, including in respect of personal health information.

The *Progressive Discipline Policy* addresses the following:

- The investigation of disciplinary matters
- The types of discipline that may be imposed
- The factors that must be considered in determining the appropriate discipline and corrective action
- The retention of documentation related to the discipline and corrective action taken

Organizational and Other Documentation

Privacy Governance and Accountability Framework

Ontario Health has developed and maintains a *Privacy Governance and Accountability Framework* for ensuring compliance with *PHIPA* and its regulation, and for ensuring compliance with the privacy policies, procedures and practices implemented by Ontario Health.

The *Privacy Governance and Accountability Framework* addresses the following:

- Accountability for compliance
- Individuals, committees and teams that support the privacy program
- Updates of board of directors
- Communication of privacy governance and accountability framework
- Relationship to security governance and accountability framework

Security Governance and Accountability Framework

Ontario Health has developed and maintains a document titled *Information Security Program Governance* for ensuring compliance with *PHIPA* and its regulation, and for ensuring compliance with the security policies, procedures and practices implemented by Ontario Health.

The document titled *Information Security Program Governance* addresses the following:

- Accountability for compliance
- Individuals, committees and teams that support the security program
- Updates of board of directors
- Communication of security governance and accountability framework
- Relationship to privacy governance and accountability framework

Ontario Health uses corporate dashboards to monitor the performance and impact of its programs.

Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Security Program

Ontario Health has established the following terms of reference (ToR) for committees that have a role in respect of its privacy and/or the security program:

- Cyber Security Steering Committee ToR
- Digital Leads Table ToR

- Enterprise Risk Management Oversight Committee ToR
- Privacy Program Advisory Committee ToR
- Information and Transformation Committee ToR
- Cyber Security Working Group ToR
- Connecting Security Committee ToR

Corporate Risk Management Framework

Ontario Health currently uses a decentralized approach to managing risks across the enterprise. Risks are managed by each portfolio/region within the organization. Each portfolio/region is required to implement its own risk management process, including maintaining a risk register, and risks are evaluated by standard criteria to determine whether they should be escalated to the *Enterprise Risk Register*.

The *Privacy Risk Management Policy and Procedures* establishes the risk management framework for the Privacy portfolio whereas the *Information Security Risk Management Standard* establishes the risk management process for security risks.

The IPC is of the view that while the Manual contemplates a single risk management framework and risk register, the process described by Ontario Health for separate portfolio/regional risk management frameworks and risk registers that feed into the enterprise level risk management framework and risk register is acceptable and appropriate given the size and complexity of Ontario Health's operations.

However, it is not clear in all respects how the portfolio/regional risk registers and risk management processes are standardized, connected to, and feed into the *Enterprise Risk Management and Governance Framework*. Furthermore, Ontario Health's risk management program would be improved with greater consistency and clarity within and among the following documents:

- *Enterprise Risk Management and Governance Framework*
- *Enterprise Risk Management Policy*
- *Privacy Risk Management Policy and Procedures*
- *Information Security Risk Management Standard*
- *Information Security Program Governance*

Ontario Health's risk management program is still evolving. As stated in the *Enterprise Risk Management and Governance Framework*: "the implementation of this framework will be an iterative process in recognition that enterprise risk management maturity is a journey that will evolve as Ontario Health progresses towards executing its target operating model and organizational structure." The IPC appreciates that Ontario Health is a new organization whose policies and procedures have not yet reached maturity. The IPC has requested Ontario Health to continue to consult with our office after the end of the review period as its risk management program matures.

Recommendation:

Continue to consult with the IPC as Ontario Health further develops its risk management policies, practices and procedures to ensure comprehensive and consistent processes, communication and escalation of privacy and security risks within and across the organization.

Corporate Risk Register

The minimum content of the *Enterprise Risk Register* is set out in Appendix 3 of the *Enterprise Risk Management Framework*. Additionally, the minimum content of the *Privacy Risk Register* is set out in Appendix A of the *Privacy Risk Management Policy* and the minimum content of the *Security Risk Register* is set out in section 2.4 of the *Information Security Risk Management Standard*. The minimum contents described meet the requirements of the Manual.

Policy and Procedures for Maintaining a Consolidated Log of Recommendations

Ontario Health has developed and maintains policies and procedures that set out the requirement and process for the following privacy and security recommendations to be logged, tracked and monitored:

- Recommendations arising from Privacy Impact Assessments (PIAs);
- Recommendations arising from Threat and Risk Assessments (TRAs);
- Recommendations arising from privacy audits and security audits;
- Recommendations arising from the investigation of:
    - Privacy Incidents;
    - Privacy Complaints; and
    - Security Incidents.
- Recommendations made by the IPC that must be addressed by Ontario Health.

Ontario Health does not maintain a separate consolidated log for all privacy and security related recommendations. However, as described below, the IPC is satisfied that the objectives of the Manual are met by Ontario Health's practices regarding its privacy and security logs.

Consolidated Log of Recommendations

Ontario Health does not maintain a separate consolidated log for all privacy and security related recommendations. Due to their infrequency, Ontario Health has indicated that recommendations that are not related to a risk are, nevertheless, tracked in the portfolio/regional risk register. On a quarterly basis, risks and recommendations are reviewed to identify and discuss a coordinated approach to addressing the risks and recommendations that may impact both privacy and security functions of Ontario Health. The IPC accepts that this approach satisfies the objectives of the Manual's requirements relating to maintaining a consolidated log of recommendations.

Appendix A of the *Privacy and Security Log of Recommendations Standard* provides reference to the corresponding policies that describe the maintenance of logs that meet the requirements of the Manual related to a consolidated log of recommendations.

Business Continuity and Disaster Recovery Plan

Ontario Health currently manages and protects the availability of its information technology environment and continuity of business functions using a decentralized approach whereby these functions are supported through a number of disparate policies and procedures, including:

- **IT Service Continuity (ITSC) / Individual Disaster Recovery Plans** that outline the specific procedure, support personnel and target timeline to resume critical operations at a secondary location in the event of a major incident (disaster) rendering the primary location inoperable; currently there are 120 documented ITSC plans available in the operational library.
- **Incident Management** policy and processes that control the identification, triage and resolution of information technology service impacting incidents.
- **Service Transition** processes that ensure all services have documented support models, support personnel, ITSC plans, monitoring and the identification and assignment of any risks to availability.
- **Change Management** policy and processes that protect the availability of the IT environment during change activity including scheduling, identification of stakeholders, and approval and notification of planned changes to external users.
- **Service Asset and Configuration Management** policy and procedures that manage the capture of information in the IT service management system to support the above processes.
- **Business Continuity and Crisis Management Program** that includes policy and standards that describe business continuity responsibilities, audit, and testing criteria to ensure continuity of Ontario Health processes and staff safety in case of an event that impacts Ontario Health's ability to deliver its critical products and services.

While these policies, procedures and processes likely contain most of the elements the IPC would expect as part of a business continuity and disaster recovery plan, as presented, they do not constitute a comprehensive and consolidated plan. The IPC appreciates the challenges inherent in managing the complex technological infrastructure needed to develop and maintain the EHR. This complexity underscores the imperative to have in place a consolidated and comprehensive business continuity and disaster recovery plan that ensures the continued protection of the personal health information managed by Ontario Health in the event of disaster or other business disruption.

Ontario Health has indicated that an overarching business continuity and disaster recovery plan that would document a consistent Business Continuity and IT Service Continuity Policy and Framework for Ontario Health regardless of solution, location or purpose is to be developed as part of Ontario Health's transformation activities. On September 15, 2021, the IPC was provided with a project plan with a detailed schedule to complete the development of a comprehensive and consolidated enterprise-wide business continuity and disaster recovery plan. The plan indicates that this work will be completed by September 30, 2022 and will be provided to the IPC before October 31, 2022. Ontario Health will continue to consult with the IPC as this work progresses.

Recommendation:

Provide the IPC with a draft comprehensive and consolidated business continuity and disaster recovery plan for review and comment before the start of the next review period.

Indicators

Ontario Health provided the IPC with indicators pursuant to the requirements of the Manual for the purpose of this initial review of Ontario Health as a prescribed organization. The indicators span the time period of October 1, 2020 to June 1, 2021 unless otherwise specified. The following is a summary of the IPC's review of these indicators.

Privacy Indicators

General privacy policies, procedures and practices

During the period of October 1, 2020 to April 1, 2021 (indicator period), all policies, procedures and practices relevant to the review of Ontario Health as the prescribed organization were reviewed by Ontario Health to meet the requirements of its initial review as the prescribed organization. The information provided to the IPC regarding these reviews meets the requirements for this indicator as set out in the Manual.

Receiving personal health information

The descriptions of the types of personal health information received by Ontario Health within all repositories (six in total, **as described above**) were reviewed in preparation for the initial review of Ontario Health as the prescribed organization. Minor edits were made for clarity (no amendments were made to the types of personal health information as a result of the review).

Managing consent in the EHR

During the indicator period, there were 278 instances in which a consent directive was made, modified or withdrawn.

Ontario Health does not log instances in which a notice of a consent directive has been provided to a health information custodian in accordance with subsection 55.6 (7) of *PHIPA*, therefore Ontario Health was unable to supply the IPC with the information that would satisfy this indicator. However, **as noted above**, it is the IPC's view that Ontario Health utilizes an adequate alternative process to having a log of notices of consent directives in place and, therefore, the IPC is satisfied that Ontario Health is able to meet the objective of this requirement without providing a specific number.

During the indicator period, there were 1,988 consent overrides performed. Of those, 1,917 were performed on the basis of express consent (as per subsection 55.7 (1) of *PHIPA*). The remaining 71 consent overrides were performed on the basis of a risk of harm to the individual or on the basis of a risk of harm to another person or group of persons (pursuant to subsections 55.7 (2) and (3) of *PHIPA*). All 71 consent overrides were conducted in respect of the acCDR.

Currently, Ontario Health's log of consent directives does not differentiate between a consent override performed on the basis of a risk of harm to the individual (subsection 55.7 (2)) versus where the consent directive is performed on the basis of a risk of harm to another person or group of persons (subsection 55.7 (3)). This is the subject of a recommendation **as described above**.

Pursuant to paragraph 16 of section 55.3 of *PHIPA*, Ontario Health is required to submit to the IPC, at least annually, a report that includes information that Ontario Health is required to keep regarding all instances of consent overrides. The IPC accepts that the information provided for the purposes of this indicator satisfies the requirements for its first annual report pursuant to paragraph 16 of section 55.3 of *PHIPA*. The next report will be received by the IPC within one year following October 1, 2021.

During the indicator period, Ontario Health received eight requests from health information custodians pursuant to paragraph 9 of section 55.3 of *PHIPA* for the electronic records of consent directives and consent overrides. In the same period there were no requests from the IPC pursuant to paragraph 8 of section 55.3 for the electronic records of consent directives and consent overrides.

Viewing, handling or otherwise dealing with personal health information

During the indicator period, 62 Ontario Health employees or other persons acting on behalf of Ontario Health were granted application access, and 120 employees or other persons acting on behalf of Ontario Health were granted operational access to view, handle or otherwise deal with personal health information. Application access includes access directly to the EHR application that hosts records of personal health information. Operational access includes access for maintaining and monitoring the back-end systems that host the EHR applications, where there is potential exposure to personal health information.

Provision of personal health information pursuant to sections 55.9 (3) or 55.10 (1) of *PHIPA*

During the indicator period there were no directions issued pursuant to sections 55.9 (3) or 55.10 (1) for any provision of personal health information that is accessible by means of the EHR.

Access and correction

As section 51 (5) of Part V of *PHIP*A has not yet been proclaimed, no access and correction decisions have been made by Ontario Health in its capacity as the prescribed organization.

As noted above, Ontario Health facilitates access and correction requests pursuant to its policies and procedures approved in accordance with paragraph 18 of section 55.3 of *PHIP*A. Ontario Health does not release records directly to the requester nor make any access/correction decisions under *PHIP*A. Health information custodians that are public sector institutions have reporting obligations to the IPC, related to access and correction requests, as part of their annual statistical reporting.

Agreements with third party service providers

No new agreements have been executed with third party service providers with access to personal health information from the period of October 1, 2020 to June 1, 2021. This does not include renewal of existing agreements.

Privacy impact assessments

During the indicator period there were nine PIAs completed by Ontario Health. The information provided to the IPC regarding these PIAs meets the requirements for this indicator as set out in the Manual.

During the indicator period there were five PIAs that were undertaken but not completed. Each PIA will be completed prior to go-live of the project.

There were four PIAs that were identified as not having yet been undertaken. Each PIA will be completed prior to go-live of the project in 2022.

There was one determination that a PIA was not required. This determination was made because the project did not involve the collection, use or disclosure of personal health information nor a change to safeguards.

The IPC was not consulted on any of these PIAs during the indicator period.

Privacy audit program

Ontario Health continuously monitors all electronic records (audit events) that Ontario Health is required to maintain in relation to consent directives and consent overrides through information and event monitoring applications.

Ontario Health conducts audits of the electronic records that Ontario Health is required to maintain in relation to consent directives and overrides if:

- There is an alert generated through the information and event monitoring systems that has been reviewed and requires investigation (i.e. constitutes a privacy incident/suspected breach);
- There is a privacy incident, risk or complaint identified or raised in relation to a consent directive or override; or
- There is an audit scheduled in accordance with Ontario *Health's Privacy Audit and Compliance Policy*, and the *Privacy Audit Schedule*, to assess compliance with Ontario Health's privacy policies, procedures, and practices that requires review of these electronic records.

No audits of this nature were required or conducted during the time period from October 1, 2020 to June 1, 2021.

Ontario Health started a privacy audit of compliance with privacy policies on May 15, 2021 and completed the audit on June 29, 2021. No recommendations were made.

Ontario Health started a privacy audit of access permissions to personal health information in June 2020 and completed the audit in July 2020. It was recommended that privileged access be revoked for individuals identified as no longer requiring access. That access was revoked in July 2020.

Ontario Health continuously conducts privacy audits of access permissions to personal health information.

Privacy breaches

All privacy breaches

During the indicator period there were 19 notifications of actual and suspected privacy breaches received by Ontario Health – ten were actual breaches of personal health information, two were suspected breaches of personal health information, and the remaining seven were breaches of policies and procedures.

Privacy breaches caused by one or more health information custodians

Of the total breaches, during the indicator period there were ten actual breaches of personal health information and one suspected breach of personal health information caused by one or more health information custodians. There were seven breaches of policy caused by one or more health information custodians.

Breaches of personal health information caused by Ontario Health

During the indicator period there was one suspected breach of personal health information caused by the prescribed organization or a system that retrieves, processes or integrates personal health information in the EHR. The information provided to the IPC regarding the suspected breach meets the requirements for this indicator as set out in the Manual.

Breaches of personal health information caused by a third party

During the indicator period there were no actual, suspected or policy breaches caused by a person who is not an employee or other person acting on behalf of Ontario Health or an agent or electronic provider of a health information custodian.

Privacy complaints

During the indicator period there were four privacy complaints received by Ontario Health. Three of those privacy complaints were investigated by Ontario Health. The privacy complaint that was not investigated required further details in order to investigate; however, the individual did not provide any contact information for follow-up.

The information provided to the IPC regarding the privacy complaints meets the requirements for this indicator as set out in the Manual.

Security Indicators

General security policies and procedures

During the indicator period, all policies, procedures and practices relevant to the review of Ontario Health as the prescribed organization were reviewed by Ontario Health to meet the requirements of this initial review of Ontario Health as the prescribed organization. The information provided to the IPC regarding these reviews meets the requirements for this indicator as set out in the Manual.

Physical security

During the indicator period, two audits were conducted of employees and other persons acting on behalf of Ontario Health granted approval to access the premises and locations within the premises where records of personal health information are retained.

During the first audit in October 2020, it was observed that several access cards were not returned to the Facilities department when no longer required (i.e., termination, leaves, etc.). The risk was low as the offices were closed and employees were prevented from accessing the offices due to the COVID-19 stay at home order. It was recommended that access cards be deactivated and that a unified access card procedure be created that requires quarterly audits of access cards. These recommendations have been addressed.

During the second audit in May 2021, it was identified that access cards for staff on leave were not retrieved because the Facilities department had not been notified of the leave. It was recommended that the Facilities department consistently receive off-boarding notification. As of September 17, 2021, Ontario Health's Human Resources has updated its notification process accordingly.

Acceptable use agreements

While Ontario Health has an *Information Acceptable Use Policy* and employees and other persons acting on behalf of Ontario Health are required to comply with all applicable policies, there was no Ontario Health *Acceptable Use Agreement* in effect during the reporting period. Thus, no employees or other persons acting on behalf of Ontario Health acknowledged and agreed to a specific *Acceptable Use Agreement*.

Ontario Health will deploy an *Acceptable Use Agreement* across the organization and will include the related indicator for the next reporting period.

End user agreements

Ontario Health has signed 840 agreements with health information custodians to collect personal health information from the EHR during the indicator period. Ontario Health has also signed six agreements with health information custodians to provide personal health information to the EHR during the indicator period. These agreements include provisions related to compliance of the health information custodians' end users. **As discussed above**, Ontario Health does not currently enter into agreements with every end user.

Security audit program

During the period of October 1, 2020 to May 31, 2021, Ontario Health received 238 requests from health information custodians for electronic records that Ontario Health is required to keep pursuant to paragraph 4 of section 55.3 of *PHIP*A.

There have been no requests received from the IPC pursuant to paragraph 8 of section 55.3 for the electronic records that Ontario Health is required to keep pursuant to paragraph 4 of section 55.3 of *PHIP*A.

Ontario Health continually audits and monitors, through auditing and event monitoring tools, all electronic records that Ontario Health is required to keep under paragraph 4 of section 55.3 and to audit and monitor pursuant to paragraph 7 of section 55.3 of *PHIP*A.

During the indicator period, seven security audits were conducted of all other system control and audit logs. The information provided to the IPC regarding these audits meets the requirements for this indicator as set out in the Manual.

Threat and risk assessments

During the indicator period two TRAs were completed. The information provided to the IPC regarding these TRAs meets the requirements for this indicator as set out in the Manual.

Information security breaches

During the indicator period, there were five notifications of security breaches or suspected breaches received by Ontario Health. Of those, three were identified as security breaches. No security breaches were caused by one or more health information custodians. Two of the breaches were caused by Ontario Health or a system that retrieves, processes or integrates personal health information in the EHR. The remaining breach was caused by a person who is not an employee or other person acting on behalf of Ontario Health or an agent or electronic service provider of a health information custodian. The information provided to the IPC regarding these information security breaches meets the requirements for this indicator as set out in the Manual.

Human Resources Indicators

Privacy and security training and awareness

During the period of October 1, 2020 to June 1, 2021, 107 employees and other persons acting on behalf of Ontario Health completed EHR initial/role-based privacy and security training. No employees or other person acting on behalf of Ontario Health who may have access to personal health information that is accessible via the EHR have yet to take their initial/role-based EHR privacy and security training.

Ontario Health's organization-wide deployment of annual (ongoing) privacy training was currently in progress at the time the indicators were reported with 1,978 employees and other persons acting on behalf of Ontario

Health having completed the course, and 854 outstanding employees and persons acting on behalf of Ontario Health that were in progress/enrolled to complete the course.

Ontario Health's organization-wide deployment of annual (ongoing) security training was currently in progress at the time the indicators were reported with 1,869 individuals having completed and 986 outstanding individuals in progress/enrolled to complete the course.

As the training campaign was still underway at the time the indicators were reported, it is expected that all employees and other persons acting on behalf of Ontario Health will have completed these courses by October 15, 2021.

This indicator does not include employees and other persons acting on behalf of Ontario Health from the Patient Ombudsman Office who received separate privacy training specific to the Patient Ombudsman's Office. These individuals are not granted approval to access personal health information that is available through the EHR.

Ontario Health described four communications to employees and persons acting on behalf of Ontario Health in relation to privacy and security. The information provided to the IPC regarding these communications meets the requirements for this indicator as set out in the Manual.

Confidentiality agreements

During the period of October 1, 2020 to June 1, 2021, 14 employees and other persons acting on behalf of Ontario Health from the Digital Excellence in Health portfolio (the portfolio that is accountable for the development and maintenance of the EHR) have executed the *Confidentiality Agreement*. No employees or other persons acting on behalf of Ontario Health from this portfolio who have commenced employment, contractual or other relationships with Ontario Health have yet to execute the *Confidentiality Agreement*.

Termination or cessation

During the period of October 1, 2020 to June 1, 2021 Ontario Health received 157 notifications from employees or other persons acting on behalf of Ontario Health related to termination of their employment, contractual or other relationship with Ontario Health. 29 of these were from the Digital Excellence in Health portfolio which is the branch of Ontario Health that is responsible for the EHR. The remaining 128 notifications were from employees or other persons acting on behalf of Ontario Health in other portfolios.

Organizational and Other Documentation Indicators

Risk management

During the indicator period the *Enterprise Risk Register* was reviewed three times: in October 2020, January 2021 and April 2021. The first two reviews did not result in any material amendments to the *Corporate Risk Register*. The review in April 2021 resulted in an amendment to reflect and align with board-identified risks.

Business continuity and disaster recovery

During the indicator period, disaster recovery was tested via a table-top exercise on November 5, 2020. On a daily basis, Digital Excellence in Health validates all previous day's backups that were successfully completed. In addition, a backup restore test for four of the repositories occurred within the indicator period.

The Business Crises and Continuity Management (BCCM) team holds yearly mini tabletop tests with all departments for the Digital Excellence in Health portfolio. During the indicator period, 15 tests were conducted across the enterprise.

With regard to disaster recovery, the new connectivity method Fast Healthcare Interoperability Resources (FHIR) service for one EHR system was added.

With regard to business continuity, no changes or amendments were made to business and continuity plans as a result of the testing.

Summary of Recommendations

Before the start of the next review period it is recommended that Ontario Health:

1. Consent Management

   a. Provide the IPC with a detailed plan, complete with timelines, that ensures the timely implementation of a mechanism to enable all health information custodians to perform a consent override pursuant to subsections 55.7 (1)-(3) of *PHIPA* when attempting to access personal health information within the DI-CS repository.
   b. Continue to consult with the IPC to address the circumstances where a consent override is not currently possible pursuant to subsection 55.7 (2) or (3) of *PHIPA*, including when attempting to access personal health information within the Ontario Laboratory Information System (OLIS) and the Digital Health Drug Repository (DHDR).
   c. Provide the IPC with a detailed plan, complete with timelines, for implementing expanded functionality within the ConnectingOntario clinical viewer to ensure that health information custodians accessing the electronic health record through this method are able to distinguish whether a consent override is being conducted for the purposes of subsection 55.7 (2) or (3) of *PHIPA*.
   d. Until all health information custodians have the functionality to perform consent overrides (for the purposes of section 55.7 of *PHIPA*) for all repositories within the electronic health record, take reasonable steps to ensure that individuals who request a consent directive and have previously requested a consent directive are provided with notice that consent overrides may not be possible in the circumstances described above so that they are aware of the risks. It is further recommended that Ontario Health continue to consult with the IPC regarding the notice before implementation.

2. Risk Management Program

   Continue to consult with the IPC as Ontario Health further develops its risk management policies, practices and procedures to ensure comprehensive and consistent processes, communication and escalation of privacy and security risks within and across the organization.

3. Business Continuity and Disaster Recovery Plan

   Provide the IPC with a draft comprehensive and consolidated business continuity and disaster recovery plan for review and comment before the start of the next review period.

4. End User Agreements

In consultation with the IPC:

   a. Develop a proposal and accompanying plan that provides assurance that all health information custodians and coroners have implemented an acceptable method for receiving an acknowledgement and agreement from end users to comply with the privacy and security obligations set out in the agreements between Ontario Health and health information custodians and coroners on a regular basis (at least annually).
   b. Ensure that the proposal and plan, described above, provides assurance that health information custodians and coroners are keeping track of these acknowledgements in a manner that can be easily audited by health information custodians, coroners and Ontario Health.

Statement of IPC Approval of Practices and Procedures

The IPC is satisfied that Ontario Health has in place practices and procedures for the purpose of protecting the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. Accordingly, effective October 1, 2021, the practices and procedures of Ontario Health have been approved by the IPC. However, Ontario Health will continue to consult with the IPC, after October 1, 2021, toward addressing the recommendations described above and as Ontario Health's policies, practices and procedures are further developed.

In order to synchronize the timing of the IPC's review of Ontario Health as the prescribed organization with its other reviews of Ontario Health as a prescribed entity and prescribed person, this approval will remain in effect until October 31, 2023.

Review of Ontario Health: The Prescribed Organization under the *Personal Health Information Protection Act*

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

October 2021