2022/23 Ontario Health Annual Privacy and Security Report

Ontario Health

Contents

1. Introduction 3

2. Background 4

3. Key Privacy and Security Milestones and Achievements 9

4. Key Program and Project Initiatives 15

5. Privacy and Security by the Numbers: Key Metrics 20

6. Looking Forward 24

Appendix A – Acronyms 27

1. **Introduction** *(updated)*

Ontario Health is an integrated agency of the Ministry of Health with a mandate to transform, connect and coordinate our province's health care system to help ensure that Ontarians receive the best possible care. This includes providing information, digital tools and services to the Ministry of Health, health care providers, and organizations across the health care sector in Ontario that are needed to put people and patients first, improving their health care experience and their health outcomes closer to home.

To meet its mandate, Ontario Health requires access to data, including personal health information (**PHI**) and personal information (**PI**), from organizations and individuals throughout Ontario. When handling this information, Ontario Health is subject to the *Personal Health Information and Protection Act* (**PHIPA**) and the *Freedom of Information and Protection of Privacy Act* (**FIPPA**) and is committed to respecting the privacy rights of individuals, safeguarding their information and complying with Ontario's privacy laws.

The coordination and expansion of connected privacy enabled digital health solutions, responsible use of data and data protection at Ontario Health is complex, exciting, and rapidly evolving. Together with the modernization of privacy legislation, they can positively impact Ontarians, including health outcomes. Whether it is strategies to give Ontarians better access to their health data or ensuring privacy rights are upheld, establishing a privacy and ethical framework for the use of machine learning and artificial intelligence in research, reviewing vendor information practices, supporting the modernization of PHIPA or anchoring data governance and management, the work of the Ontario Health Privacy Office and Information Security teams have meaningful and tangible impact. It builds trust, fosters innovation and enables Ontario Health to deliver on its key strategic priorities.

A wise physician once said, "If patients believe they are getting good care, they are getting good care. If patients believe they are getting bad care, they are getting bad care".

Likewise, if patients believe that the most sensitive information about them is not protected, they may withhold that information which in turn could impact their care. If health care providers have concerns about Ontario Health's ability to protect the billions of data assets it holds, then this too could impact the care of Ontarians. Ontario Health's approach to privacy and security fosters confidence and helps ensure Ontarians receive the best possible care.

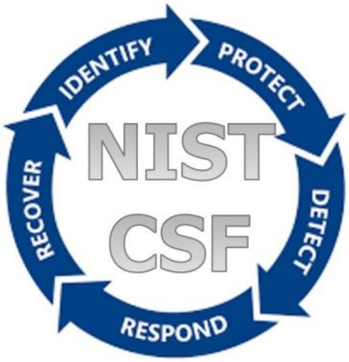
In 2022/23 Ontario Health's Privacy and Information Security teams in collaboration with other business partners across Ontario Health and the province, have continued to work together to remove barriers and address new PHIPA authorities, data privacy, cybersecurity, interoperability and other compliance matters, while continuously evolving and maturing its privacy and information security programs. This Annual Privacy and Security Report describes Ontario Health's privacy and security programs and highlights milestones achieved in 2022/23 fiscal year that support and advance Ontario Health in achieving its mandate. The report also takes a look back at key metrics, some of which are reported to the Office of the Information and Privacy Commissioner of Ontario (**IPC**) and takes a look forward at privacy and security priorities for 2023/24.

2. Background

Security Program

Ontario Health is dedicated to ensuring the protection of the information and systems it designs, builds, and operates in support of delivering provincial health care services. To achieve this goal, Ontario Health has established a comprehensive risk-based Information Security Program within the Digital Excellence in Health portfolio, inclusive of physical, technical, and administrative safeguards designed to ensure a safe and secure environment for the delivery of digital health care. These safeguards are implemented in accordance with legislative requirements, international standards, and prioritized risk-based decisions. The goal of the Information Security Program is to ensure that confidentiality, integrity, and availability are provided for data and services. In alignment with the Ontario Health Privacy Program, security is considered as a fundamental design principle for all systems and digital operations, ensuring a culture of security is pervasive throughout the Digital Excellence for Health portfolio.

Governance for the Information Security Program is provided through the Vice President, Innovations in Connected Health, who reports directly to the Digital Excellence in Health Executive. The program execution and operations are led by the Information Security Office and supported across the Digital Excellence in Health portfolio by the Digital Leadership Team. The Information Security Office is accountable for the day-to-day operations of the program, including the identification, assessment, and mitigation of security risks; development and implementation of administrative controls via policies, standards, and procedures based on National Institute of Standards and Technology (**NIST**) and ISO 27001 frameworks; providing internal security advisory services; and supporting the response to incidents and breaches in conjunction with the Cyber Security Defense team.



NIST Cybersecurity Framework

Through collaboration with various internal and external stakeholders, the Information Security Program ensures that security is a key component of all system implementation phases, from inception to implementation and operations.

Privacy Program

Ontario Health is committed to respecting personal privacy and safeguarding the PHI and PI that it has in its custody or control. To support this commitment, Ontario Health has a robust fit for purpose privacy program designed to ensure a privacy culture is not only established but also anchored across the agency allowing it to operate in accordance with its legal obligations and responsibilities. Ontario Health believes that legislation is the floor and not the ceiling for driving compliance. As such it maintains as a foundation 'Privacy by Design' principles and industry standards, that help build trust and foster innovation. Ontario Health must continuously earn and maintain the trust and confidence of Ontarians as well as its key stakeholders and partners in order to fulfill its mandate.

Ontario Health's privacy governance and accountability structure provides assurance that the management of its privacy program is monitored and aligned with its objectives and legal framework. The program resides within the Legal, Privacy, Risk and Governance portfolio whose mission is to uphold public trust by providing valuable advice in compliance and risk management. The privacy program is led by the Chief Privacy Officer (**CPO**), who reports directly to the General Counsel and Executive Lead of the Legal, Privacy, Risk and Governance portfolio. A team of dedicated privacy professionals, managers and a director support the CPO in managing the day-to-day operations of Ontario Health's privacy program, including collaborating with the Ministry of Health, the IPC, and other provincial stakeholders, identifying and mitigating privacy risks; vendor management, supporting new data acquisitions and uses, leading policy development initiatives; overseeing privacy training, managing consent directives, privacy breaches, access, and correction requests.

In partnership with its information security and other business partners across all portfolios, the Privacy Office provides operational, advisory and assurance services that include risk-based, pragmatic, and creative privacy solutions. These solutions enable portfolios and programs to meet annual business plan objectives while minimizing residual risk to the organization. Because of these close partnerships, privacy requirements and controls are embedded in new projects, processes, and programs in ways that facilitate Ontario Health's ability to fulfill its mandate while protecting the privacy rights of Ontarians.

Privacy Legislation

Ontario Health derives its mandate and authority to collect, use, and disclose PHI and PI from its designations under Ontario's PHIPA, FIPPA, the *Gift of Life Act* and the *Connecting Care Act*. The following list describes the various privacy legal authorities which Ontario Health relies upon for its operations and to optimize its permitted use of date for good:

Prescribed Entity (PE)
Ontario Health is designated as a ‘prescribed entity’ for the purposes of subsection 45(1) of the PHIPA. Subsection 45(1) of PHIPA permits health information custodians (such as hospitals, laboratories and physicians) to disclose PHI without consent to Ontario Health as a prescribed entity for the purpose of analysis or compiling statistical information with respect to the management, evaluation or monitoring of the allocation of resources to or planning for all or part of the health system, including the delivery of services (‘health system planning and management’). For example, collecting and using PHI as a prescribed entity enables Ontario Health’s Ontario Renal Network (**ORN**) to conduct capacity planning analysis for renal services offered by Ontario’s regional renal programs.

Prescribed Person (PP)
Ontario Health is also designated as a ‘prescribed person’ for the purposes of subsection 39(1)(c) of PHIPA with respect to its role in compiling and maintaining two prescribed registries under subsection 13(1) of O. Reg. 329/04: i) the Ontario Cancer Screening Registry (**OCSR**), and ii) the CorHealth registry of cardiac and vascular services. This designation grants Ontario Health the authority to collect, use and disclose PHI in these registries for the purposes of facilitating or improving the provision of health care.

Prescribed Organization (PO)
On October 1, 2020, the Government of Ontario designated Ontario Health as a ‘prescribed organization’ further to the enactment of Part V.1 of PHIPA. This represents a change in legal authority for Ontario Health and builds on the operational and privacy framework that was originally put in place under section 6.2 of Ontario Regulation (**O. Reg.**) 329/04 in December 2011, to maintain the electronic health record (**EHR**) and will, in future, support new uses of the EHR.

The EHR is comprised of the provincial client and provider registries, laboratory, prescription drug, diagnostic imaging (common services), and clinical documents received from health information custodians such as hospitals and family health teams. As a prescribed organization, Ontario Health enables access to PHI to authorized health care providers, for the provision of healthcare for example, through the ConnectingOntario application. Ontario Health is also permitted to enable access to PHI to coroners and medical officers of health for other authorized uses.

PHIPA Agent
The definition of agent in PHIPA includes any person (including organization, such as Ontario Health) who is authorized by a health information custodian to perform services or activities in respect of PHI on the custodian’s behalf and for the purposes of that custodian. As a PHIPA Agent, Ontario Health is authorized to facilitate patient access and correction requests for their PHI in EHR.

Researcher
Ontario Health operates a research program to develop new knowledge through epidemiological, intervention, health services, surveillance, and policy research, as well as knowledge synthesis and

dissemination. Ontario Health can use PHI it collected as a prescribed entity or a prescribed person for the purposes of research, subject to restrictions and conditions set out in PHIPA.

Electronic Service Provider (ESP) and Health Information Network Provider (HINP)

Ontario Health provides electronic information services to health information custodians to enable them to collect, use, modify, disclose, retain, or dispose of PHI, and/or to exchange PHI with each other. In providing such services, Ontario Health is acting as an ESP and/or HINP, pursuant to O. Reg. 329/04, s. 6 (1) and 6(2) of PHIPA. These roles strictly limit Ontario Health's use of PHI to that which is required to support electronic services to custodians. Ontario Health provides many application services as a HINP, including the Client Health and Related Information System (**CHRIS**), as well as eConsult technology that enable health care providers and organizations to share PHI for health care purposes.

FIPPA Institution

Ontario Health is an 'institution' as defined in FIPPA and is subject to its provisions. FIPPA regulates the collection, use, disclosure, and retention of personal information. Ontario Health's collection of personal information directly from a patient, for example, as part of the Patient and Family Advisor Network, is subject to the restrictions set out in FIPPA. FIPPA also provides the public with a right of access (e.g.,, through Freedom of Information or '**FOI**' requests) to records in the custody or under the control of an institution.

Gift of Life Act

Trillium Gift of Life Network (**TGLN**), a part of Ontario Health, collects, uses, and discloses personal information, including personal health information, for the purposes of planning, coordinating, supporting, researching, and reporting on all aspects of organ and tissue donation and transplantation. This handling of personal information is authorized by the *Gift of Life Act*, which permits TGLN to, directly or indirectly, collect information about individuals for the purpose of organ and tissue donation and transplantation. Further, the Act provides the agency with the authority to use and disclose personal information with certain individuals, specifically designated facilities or enter into data sharing agreements with other organizations provided appropriate confidentiality mechanisms are in place.

Changing Regulatory Landscape

Since 2019, the Ministry of Health has taken significant steps to consult with stakeholders in the healthcare sector to "modernize" PHIPA. Some of the drivers of change have been the acceleration of digital and virtual care and supporting patient's rights to digitally access records. These changes directly impact Ontario Health and the many important roles it plays in supporting how data can be used for the benefit of all in improving patient care.

PHIPA Modernization Consultations *(updated)*

Over the past year, Ontario Health welcomed the opportunity for consultation on proposed changes to PHIPA, working closely with its stakeholders, including the Ministry of Health as part of the Dialogue on Data. As part of these consultations, Ontario Health identified, challenged and proposed ways to modernize PHIPA that both reflect the complexity of Ontario's health system and also increases the capacity for data sharing to enable the provision of integrated and improved health care to Ontarians. Feedback compiled through the Ministry's Dialogue on Data consultations will be used by the Ontario Health Data Council to formulate recommendations on improvements to PHIPA.

Electronic Health Record *(updated)*

Due to the growing demand from individuals for digital access to their own health records, the Ontario Government introduced regulatory changes to enable Ontario Health, as the prescribed organization, to provide individuals with access to their PHI from the EHR through digital means specified by Ontario Health. The regulations, not yet in force, would allow Ontario Health to phase in this digital access over time, starting with digital access to their health records contained in the Ontario Laboratories Information System (**OLIS**) and Digital Health Drug Repository (**DHDR**).

Right to Access Personal Health Information in Electronic Format[1] *(new)*

Pursuant to PHIPA, individuals have the right to access their records of PHI in the custody or control of health information custodians, subject to limited exceptions. In 2022, the government amended PHIPA to provide individuals with a right to access a record of PHI *in an electronic format* that meets any requirements that may be prescribed, or an electronic format specified by Ontario Health in accordance with the PHIPA regulation. These changes will allow for electronic formats to be prescribed that are up-to-date and based on standards, allowing for patients to better access and use their data to manage their health status and health care journey.

IPC's Review Process and Manuals for the Review and Approval of Prescribed Entities, Prescribed Persons and Prescribed Organizations *(new)*

In 2021, the IPC released proposed updates to the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities, which includes updates to both policy requirements as well as the review process. The IPC is looking to implement a more risk-based approach to their review process.

After conducting a thorough review of the proposed changes and consulting with affected Ontario Health business teams, the Privacy Office and Information Security team collaborated with other prescribed entities and prescribed persons to submit joint comments and proposed

[1] Government Notices — Other | Ontario Gazette Volume 155 Issue 39 | September 24 2022 | ontario.ca

recommendations to the IPC that focused on usability and alignment with standards. While the new review process is in effect for the current review process, the draft policy requirements have yet to be finalized.

3. Key Privacy and Security Milestones and Achievements

In 2022/23, the privacy and security teams focused on achieving the following goals.

Ontario Health Data Council – Digital Citizens Working Group *(updated)*

Established in 2021, the Ontario Health Data Council (**OHDC**) provides advice to the Minister of Health on the strategic management of Ontario's health data to foster a person-centred learning health system. Ontario Health's Population Health and Value Based Health System's Executive participates as a member of the OHDC in advising on the management of the integration of Ontarians' health data to generate analytics, insights, and innovations needed by the health care sector and government decision-makers. The OHDC also serves in the capacity of the Electronic Health Record Advisory Committee to fulfill the legislative mandate specified in section 55.11 of PHIPA. The OHDC established working groups to assist in and inform its work, including the Digital Citizen Working Group which included the CPO and Vice President Innovations for Connected Health as representatives from Ontario Health.

The Ministry website contains the following description of the OHDC report on data use for integrated care:

"In November 2022, the OHDC shared its report with the Ministry of Health on how Ontario can use data to create a more integrated healthcare system for patients. Recommendations from the OHDC Report will help the province continue leveraging data to support more connected and convenient care across Ontario. The Council has identified the following key strategic recommendations to guide the transformation of Ontario's health data ecosystem:

- Integrate and use health data to advance health and equity outcomes for people, communities, and populations
- Promote health equity through appropriate data collection, analysis, and use
- Establish system-level trustworthy governance and policies for health data as a public good
- Respect and support First Nations, Inuit, and Métis Peoples' Data Sovereignty
- Build data stewardship capacity and enable sharing by default." [2]

[2] https://www.ontario.ca/page/ontario-health-data-council-report-vision-ontarios-health-data-ecosystem

EHR Advisory Support Working Group *(new)*

The EHR Advisory Support Working Group (the Working Group) is a standing advisory body supporting and reporting to the OHDC in its EHR Advisory Committee capacity. The Working Group consists of one member of the Council acting as the Working Group's chair, and representatives of Ontario's broader health sector who have interests in the EHR and the privacy protection of PHI. These include health information custodians, the IPC, and the public as well as Ontario Health representatives in the capacity as the prescribed organization and as responsible for the management and operation of the EHR. Ontario Health representatives include the CPO, the Director Product Management and Delivery (Laboratory, Drugs & EHR Data Management) and the Manager Privacy responsible for assurance services for Ontario Health as a prescribed organization.

The EHR advisory Support Working Group Terms of Reference identify the objectives of the working group, and include[3]:

"The Working Group will develop and submit recommendations to the Council concerning the following elements of Section 55.11 in PHIPA:

(a) practices and procedures that the prescribed organization, Ontario Health, must have in place to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of the information;

(b) practices and procedures that the prescribed organization, Ontario Health, must have in place for responding or facilitating a response to a request made by an individual under Part V for a record of personal health information relating to the individual that is accessible by means of the electronic health record;

(c) the administrative, technical, and physical safeguards the prescribed organization, Ontario Health, should have in place to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of the information;

(d) the role of the prescribed organization, Ontario Health, in assisting a health information custodian to fulfil its obligations to give notice to individuals under subsections 12 (2) and 55.5 (7) in the event that personal health information that is accessible by means of the electronic health record is stolen or lost or is collected, used or disclosed without authority;

(e) the provision of notice in the event that personal health information that is accessible by means of the electronic health record is stolen or lost or is collected, used, or disclosed without authority;

(f) anything that is referred to in Part V.1 of PHIPA or in the regulations as capable of being the subject of a recommendation of the advisory committee;

(g) responses to proposals for secondary access to data in the EHR as described in section 55.10 of PHIPA; and

[3] Ontario Health Data Council EHR Advisory Support Working Group Terms of Reference, Draft 4.0

(h) any other matter referred to the working group by the Minister through the Council."

Privacy Training and Awareness – Privacy Day *(new)*

January 22nd to the 28th 2023 was Data Privacy Week, an extension of Data Privacy Day (January 28th). This is an internationally celebrated week; a way of raising public awareness about the importance of privacy and data protection while highlighting the impact technology has on our daily lives. On Friday, January 27, 2023, the IPC hosted a Privacy Day Event: *Building Trust in Digital Health Care* chaired by Ontario's Privacy Commissioner, Patricia Kosseim, and featured Ontario Health's CPO, Sylvie Gaskin as a panelist, as well as Michael Hilmer, ADM Digital and Analytics Strategy Division, Ministry of Health, Wendy Lawrence, Chief Risk, Legal and Privacy Officer St. Joseph's Healthcare Hamilton, Nyranne Martin, CPO and General Counsel, Ottawa Hospital and Ariane Siegel, General Counsel and CPO, Ontario MD. Key issues discussed included:

- Replacing faxes with more secure forms of digital communication;
- Ushering in administrative monetary penalties under Ontario's health privacy law;
- Building privacy and security resiliency against breaches and cyberattacks; and
- Fostering a privacy-respectful culture across an organization.

To further increase privacy awareness among Ontario Health employees, the privacy team, in partnership with the Information Security Office, hosted their first Lunch and Learn event with a theme entitled, "Privacy Practices at Home and at Work." This session educated attendees on some of the more common online privacy risks and provided tips and recommendations on how individuals can protect their privacy online. To demonstrate Ontario Health's commitment to protecting privacy and safeguarding PI and PHI, this event helped to foster a privacy-respectful culture and awareness across the organization while building privacy and security resiliency against breaches and cyberattacks for staff on both a personal and professional level.

Ontario Health's 2023 Review and Approval by the Information and Privacy Commissioner (IPC) and Consent Override Report *(new)*

As a prescribed person, prescribed entity and prescribed organization, Ontario Health is required to have its information practices reviewed and approved by the IPC on a regular basis. The following describes the activities that the Privacy and Security teams have undertaken over the last year, with support from business teams across Ontario Health, to obtain this approval from the IPC.

1) 2021 Ontario Health Prescribed Organization Review: Responding to IPC Recommendations
In October 2021, Ontario Health received formal approval from the IPC with regards to the prescribed organization information practices, along with four recommendations related to Ontario Health's i) Risk Management Program, ii) Business Continuity and Disaster Recovery Plan, iii) consent management practices, and iv) EHR end-user agreement requirements. Ontario Health's

privacy and security teams worked diligently with business partners across the organization to provide the IPC, in October of 2022, with a response confirming if each recommendation has been addressed and providing a detailed plan for implementing those recommendations yet to be addressed.

2) 2022-2023 IPC Triennial Review and Approval of Ontario Health's Information Practices

During the summer of 2022, the IPC began their triennial review of Ontario Health's information practices as a prescribed entity, prescribed person, and prescribed organization. This is Ontario Health's first joint review of all three prescribed authorities. As part of the review process, the Ontario Health privacy and security offices worked closely with business units across the agency to complete and submit a report of indicators that demonstrate the information practices implemented by the organization. Indicators included, for example, a list of privacy and security assessments completed, and the results of any recommendations arising from each assessment.

As part of the new risk-based triennial review process, once the IPC reviewed the indicators and, in considering past reviews and industry trends, they requested Ontario Health to provide the following policies and procedures for further review:

- Business Continuity and Disaster Recovery Plan
- Corporate Risk Management Framework
- Information Security Audits
- Information Security Breach Management
- Statement of Purpose for Data Holdings Containing PHI

Ontario Health will continue to address any questions received by the IPC, and update information practices as required throughout the review period. Final approval of Ontario Health's information practices is expected to be received by the IPC in October 2023.

3) Annual Consent Override Report for Prescribed Organizations

In accordance with PHIPA section 55.3 paragraph 6, the prescribed organization is required to maintain a record of all instances where a consent directive has been overridden by a health information custodian to access PHI in the EHR. The IPC also requires that the prescribed organization submit a consent override report to the IPC on an annual basis that includes: the health information custodian and agent name who performed the override, the date and time of the override, and the prescribed reason for the override. Ontario Health submitted its first consent override report as an approved prescribed organization on October 1, 2022, with a supplemental report on March 31, 2023, in order to capture the full fiscal year.

Ontario Health Cyber Security Centre (formerly known as the Provincial Cyber Security Program) *(updated)*

In 2021, Ontario Health established the Cyber Security Operating Model (**CSOM**). The CSOM provides a framework that enables a coordinated approach to cyber security in the province and supports the development of robust cyber security alignment across the health care sector – incorporating people, processes, data, and technology controls to identify, protect, detect, respond, and recover from cyber threats – and ensure that patients will have access to secure health care.

As part of this model, Ontario Health launched and funded a program to pilot six Regional Security Operation Centres (**RSOCs**) and integrate these RSOCs into the CSOM. Through the CSOM and RSOC pilots, the health care system has seen an increase in cyber security awareness and cyber security capabilities across the sector, particularly within acute-care entities. Through an independent third-party evaluation of the RSOC pilots, Ontario Health has:

- Demonstrated the CSOM's value and viability in improving the availability and resiliency of patient care, setting the foundation for its continued evolvement and improvement;
- Facilitated increased awareness of health care entities' cyber security needs, with maturity assessments revealing previously overlooked gaps;
- Empowered the RSOC pilots to advocate and implement change in their membership;
- Enabled technology and resource harmonization across the region;
- Maximized participants' savings and efficiencies through volume licensing and service sharing;
- Demonstrated the hypothesis that "cyber is a team sport" and the value of building a cyber community of thought leadership and support;
- Achieved 44% coverage of Ontario's health care providers; and
- Enabled smaller entities with much needed and rapid gains in cyber capabilities via participation in the model.

Ontario Health is leading the operationalization of the next iteration of the CSOM over the next three years to bring to life a defined vision and model for cyber security within the Ontario health care sector. 22 million dollars of funding has been approved and allocated to be spent in FY23/24 towards operationalizing the CSOM's next phase. This revised model incorporates the lessons learned and future considerations highlighted during the initial CSOM and RSOC pilot program. The new CSOM introduces a collaborative and iterative approach to cyber security that will allow for ongoing sector-wide improvements to protect patient data consistently and effectively against emerging cyber threats.

The next iteration of the CSOM will also continue to support an increase in cyber security resiliency across the sector through:

- A prescribed framework of roles and responsibilities, including expectations and requirements for all entities via the Provincial Policy Statement, Operational Directions and Standards
- Enhanced collaboration among health care entities at all levels of the system
- Greater monitoring and coverage through shared managed security services
- Implementation of CSOM standardization and evaluation via accountability agreements and performance overlays

- Membership and alignment to a Local Delivery Group (**LDG**) for the consumption of cyber security shared services and the acquisition of affiliated Managed Security Service Provider (**MSSP**) services
- Proactive and automated cyber threat information sharing via an Incident Response Notification (**IRN**) Guidance and a Cyber Threat Intelligence Sharing (**CITIX**) Platform supported by the appropriate legal and privacy frameworks.

Patients and communities across the province will benefit from a health care system that protects patient services and data and supports better health care outcomes. The next iteration of the CSOM supports the delivery of high-quality patient care across all entities within the sector – regardless of size, complexity, or location.

Cyber Security Program Testing *(updated)*

The establishment of a harmonized Ontario Health Cyber Security Program presented several opportunities to establish improved policies and practices. The incident response practices were enhanced and tested through both tabletop exercises and lessons learned from the incident response team. As part of its effectiveness and assurance capabilities, the Information Security Office initiated and conducted a thorough penetration test as a baseline assessment to measure Ontario Health's defense robustness against a hostile cyberattack incident. This test was conducted by one of Ontario Health's third-party service providers, a global leader in cyber defense.

Moving forward, Ontario Health's Information Security Program is establishing a roadmap for improving its offensive security capabilities by standing up internal and external red, purple and blue teaming services.

Harmonizing Cyber Security Maturity Assessment Practice and Framework *(updated)*

In FY22/23, Ontario Health completed the testing and implementation of a security assessment platform that brings harmonization of risk assessment requirements in Ontario within a centralized and traceable model using the NIST Cyber Security Framework (**CSF**). This model and selected technology allows Ontario Health to have an overall security maturity view of the health care sector, while reducing the number of assessments required for granting access to provincial digital assets that are hosted and managed by Ontario Health.

Information Security Program Development and Improvement *(updated)*

In FY22/23, the holistic cyber security gap assessment, and Threat Risk Assessment (**TRA**) were conducted, and the aggregations of these results enabled Ontario Health to refresh its cyber risk register. The results of this assessment also highlighted vast improvements to the holistic security posture compared to previous assessments completed in FY20/21. This work enabled the Ontario Health Information Security Program to update the Security Capability Model, which was developed based on the previous NIST framework. In addition, this work resulted in updating the detailed

Ontario Health Information Security Service Catalogue with 73 services based on the Security Capability Model and reassessing the resources required for Ontario Health's Information Security Program. This work also supports the Ontario Health Information Security Program's refreshed three-year roadmap for improving Ontario Health's overall cyber security posture.

In FY22/23, the Ontario Health Information Security Steering Committee (**ISSC**) and its five subcommittees continued providing leadership and direction on information security to the Digital Excellence in Health portfolio under the guidance of the Digital Excellence in Health executive. In the ISSC monthly meetings, Ontario Health's Information Security Office (**ISO**) and Cyber Security Defense (**CSD**) leadership provided the latest status of security initiatives and activities to improve the security posture of Ontario Health and informed executives and senior leaders from different portfolios about the latest security trends, risks and challenges that require attention.

Modernized Hybrid Security Operations Center (SOC) *(new)*

Modern attackers look for opportunities to strike all the time – regardless of business hours. In FY22/23, Ontario Health launched an effort to create a 24/7 Hybrid Security Operating Centre (**SOC**) which continually protects and defends its assets. Through partnership with an MSSP and deployment of a cloud-based Extended Detection and Response **(XDR)** toolset, threats are blocked and escalated to Ontario Health as needed to safeguard systems and data. Coverage and modernization of the newly formed Hybrid SOC and systems will continue throughout the next fiscal year. Through this engagement, Ontario Health is building, trialing, and refining its model that is currently being scaled out through the Cyber Security Centre.

As part of building XDR, the migration to a new Security Information and Event Management (**SIEM**) yielded excellent results throughout the year. By replacing the previous SIEM tool, Ontario Health has increased coverage of its assets by over 200% while only increasing costs by approximately 37%. Using the SIEM tool alongside other security systems deployed in prior years has enabled the creation of a fully functional and cloud-based XDR system, allowing the organization to confront and respond to security threats before they impact operations.

4. Key Program and Project Initiatives

The Privacy Office in collaboration with the cyber security and other business partners is responsible to protect individual privacy and the confidentiality, security, and availability of data assets and to enable the agency to use data and other assets in support of its programs and projects. A sample of these programs and initiatives are listed below.

Individual Access to Electronic Health Records (EHR) Program *(updated)*

Ontario Health has been working with the Ministry of Health to provide individuals with digital access to data held in the provincial EHR, which is developed and maintained by Ontario Health, in accordance with its prescribed organization designation. Over the course of the last year, the

Ministry and Ontario Health worked to remove policy and legal barriers to Ontario Health providing individuals with direct digital means of access to provincially managed data. At this time, direct digital access to data held in the EHR is currently unavailable to individuals.

In the past, individuals have been able to directly access select parts of their EHR via patient portals (e.g. MyChart, myUHN) not developed or maintained by Ontario Health. Once Ontario Health's new authority is proclaimed in PHIPA, this new provincial access program aims to enable Ontarians to digital access to their data held in the EHR. The regulations would allow Ontario Health to phase in digital access over time, starting with digital access to their health records in the Ontario Laboratories Information System (**OLIS**). The Ministry believes that providing individuals with digital access to their PHI in the EHR is critical to enable better care. This program is also aligned with the "Digital Access for Patients" pillar of the Ministry's Digital First for Health strategy.

Health 811 *(updated)*

Health811, formerly Health Connect Ontario (**HCO**), and formerly referred to as Health Care Navigation Service (**HCNS**) was launched by the Government in April 2022. "Health811 is a new program to connect people to nurses and other health services from anywhere at any time. Health Connect Ontario makes it easier for Ontarian to access timely care and information by phone, chat and online"[4].

Health811 acts as a one-stop 'Digital Front Door' to Ontario's health care system, offering a place where all Ontarians can access health information, advice, and initial triage to become connected to publicly funded health care services across the province and to receive guidance throughout their health care journey. Ontario Health, including members of the Privacy Office, supported the Ministry of Health during the procurement phase. The Ministry has assigned the contract to Ontario Health which is now overseeing the implementation, ongoing management, and operations/performance of this service. Acting as a PHIPA Agent of the Ministry of Health, Ontario Health, through its privacy and information security teams, has been responsible for reviewing and approving the Health811 vendor's privacy impact assessments and threat risk assessments, risk mitigation plans, policies and procedures, and incident management practices, ensuring Health811 has privacy and security controls in place acceptable to the Ministry, Ontario Health and in accordance with the agreement framework.

Ontario Health privacy and security teams are currently reviewing the delta privacy impact assessment and delta threat risk assessment conducted by a third party for Health811 and coordinating a presentation for the IPC in preparation for the Health811 release of their use of virtual visits scheduled for go-live May 30th, 2023.

[4] https://news.ontario.ca/en/release/1002095/ontario-launches-new-tool-to-connect-people-to-nurses-and-other-health-services-from-anywhere-at-any-time

Transfer of Ontario Case Costing Program to Ontario Health *(new)*

The Strategic Partnerships Table of Ministry of Health, and Ontario Health determined that oversight of the Ontario Case Costing (**OCC**) program should transfer to Ontario Health with a planned transfer date of December 1, 2022. The OCC solution supports the systemic collection of case costing across 70 existing hospitals. Case costing is an accounting method used to track costs of providing health care to patients/ clients. It is an integration of financial, clinical and utilization data at the patient level. The solution is supported by a vendor, with data management supported by Ministry of Health, and data hosted by Ontario Health (former eHealth servers). Currently, Ontario Health uses case costing to facilitate development and management of funding models and various other financial analysis.

The transfer included the following:

1) Transition of new vendor contract, this entails:
    - An activity-based case costing solution that provides facilities with the ability to track a patient’s journey through their continuum of care across different care settings and cost each episode of care within that facility and setting;
    - Related infrastructure environment to host the solution;
    - Continuing to manage existing 70 facilities hosted in this centralized provincial solution;
    - Addition of 20 new facilities to be added to solution over five years; and
    - Ontario Health acting as a PHIPA Agent of the Ministry for the OCC program (new role for Ontario Health in respect to OCC).
2) Funding over a term of five years for vendor management and the establishment and management of a Centre of Excellence (**COE**) to support OCC facilities.

Ontario Drug Benefit (ODB) Program Coverage for Clients Receiving Home and Community Care Support Services (HCCSS) from an Indigenous Organization Funded by Ministry of Health *(new)*

This Ministry of Health-led project will enable ODB access to clients receiving home care services from Indigenous Organizations funded directly by the Ministry of Health. The HCCSS’ are being leveraged to enter these clients into the Client Health-Related Information System (**CHRIS**) to enable ODB access. As these clients are not HCCSS clients, this initiative presents unique legal authorities where Ontario Health has no direct relationship with the Indigenous Organizations. A new referral type is being developed within CHRIS to identify these patients in CHRIS. The Privacy Office has been working to provide feedback to the legal authorities’ model and develop a privacy impact assessment (PIA) on the initiative. The risks and recommendations of the PIA will be shared with the Ministry of Health to ensure alignment of program goals with ability to leverage CHRIS. The Privacy Office will continue its work to finalize the PIA and subsequently respond to the risks identified from the PIA findings.

HPV Cancer Screening Implementation *(new)*

Ontario Health has initiated a large multi-year project to implement human papillomavirus (**HPV**) testing as the foundation of the cervical cancer screening program in Ontario. The Privacy Office collaborated with the Ontario Health Procurement and the Cancer Screening teams to provide input into the procurement of a laboratory service provider(s) to support the program in addition to informing vendor selection. The Privacy Office will continue to support this initiative through development, implementation, delivery and, eventually, regular operations to ensure implementation of Privacy by Design principles, identification, and remediation of risks through a formal privacy risk assessment and project collaboration, as well as privacy operations support once the updated program has launched.

Therapist Assisted Internet-Based Cognitive Behaviour Therapy (iCBT) *(new)*

The Mental Health and Addictions Center of Excellence at Ontario Health was established to support the delivery and implementation of the provincial Mental Health and Addictions strategy. A key component of achieving this strategy is providing coordinated access to mental health services by supporting access to evidence-based, short-term, cognitive behavioural therapy (**CBT**) and related approaches to Ontarians with depression and anxiety-related conditions, with no out-of-pocket costs to participants.

The program is delivered through 10 regional psychotherapy networks as a coordinated provincial program. Each network is comprised of several organizations to administer and deliver high-quality services for individuals within a defined region of Ontario. Access to the program is centralized within each network, meaning individuals are referred directly to a Network Lead Organization (**NLO**) for screening and assessment, following which individuals are directed to the service that best meets their needs.

A competitive procurement and evaluation process took place. Two vendors were selected to deliver the service. Given that PHI is being collected, used, stored, and disclosed as a function of the iCBT solution, PIAs were conducted on both vendor solutions.

CHRIS Services & Home Care Modernization *(updated)*

The Privacy Office continues to work closely with North Toronto Ontario Health Team (**NT OHT**) to take the necessary steps for NT OHT to utilize CHRIS as their central registration system to support identification, registration and tracking of NT OHT patients. The Privacy Office has been working on addressing the identified risks and recommendations in preparation for NT OHT onboarding. Deliverables being prepared will also be used to support subsequent OHT onboarding through development of flexible tools and supports.

Additionally, the Privacy Office has been providing advice on the planning towards Home and Community Care Modernization (**HCCM**), including the Leading Projects. The Leading Projects aim to build and test new models of integrated care delivery through 7 OHTs. In collaboration with the CHRIS Product Team and Legal, the Privacy Office has provided input on how to best support these initiatives within existing legislative authorities and parameters. The Privacy Office has been sharing privacy risks and considerations that need to be accounted for in the planning prior to solidifying plans for implementation.

Home and Community Care Support Services *(*HCCSS) Support *(new)*

As part of the Shared Services Memorandum of Understanding between Ontario Health and HCCSS, Ontario Health has many responsibilities to support the HCCSS. The Privacy Office has been supporting many HCCSS initiatives as part of Ontario Health's commitment to the HCCSS'.

Work includes but is not limited to:

- Developing privacy requirements to support Request for Proposals to support vendor selection for Medical Equipment Supplies (**MES)** and Negative Pressure Wound Therapy (**NPWT**);
- Conducting evaluations of MES and NPWT request for proposal submissions;
- Initiating work to support development of PIAs for new vendors and processes related to caregiver and patient surveys.

Digital Health Information Exchange (DHIEX) *(updated)*

Enabling the sharing of electronic information between Health Information Custodians is critical to providing Ontarians with efficient, integrated health care. PHIPA was amended on January 1, 2021, to facilitate interoperability between digital health assets. Under these DHIEX amendments, Ontario Health is responsible for defining interoperability requirements (including privacy and information security) for electronic systems, determining specifications, and actively working with vendors and health information custodians through a program to monitor and ensure compliance. Ontario Health is in the process of developing certification and compliance processes to ensure that vendors, health information custodians, and Digital Health Asset owners progress to standards-based provincially guided interoperability. In 2022/23, Ontario Health held consultations with the IPC regarding the eReferral/eConsult and Acute and Community Clinical Data Repository (**acCDR**) interoperability specifications and continued to provide updates to the IPC on the patient summary and mental health and addictions specifications.

Central Waitlist Management *(updated)*

Over the last fiscal year, the Health System and Performance and Support (**HSPS**) portfolio developed a provincial eReferral repository that can receive Wait 1 data, and also launched the agile-business intelligence (Health System Insights Platform) tool that provides visibility of real-time surgical waitlists for different user groups (surgeon office, hospitals, and Ontario Health Regional

Teams). These tools enable a better understanding of demand patterns and service gaps, by exposing existing surgery Wait Times Information System (**WTIS**) data. The Legal, Privacy and Information Security teams worked in close collaboration with the HSPS Portfolio to support the data acquisitions, legal agreements and controls required to enable these waitlist management services. Work continues to support the expansion of the Health System Insights Platform to provide additional health system indicators and analytics to Ontario Health business teams and stakeholders to support health system planning and management.

Mental Health & Addictions (MHA) Centre of Excellence (COE) *(updated)*

The Ministry of Health's Roadmap to Wellness entrusted Ontario Health with a key role in the delivery and quality of MHA services. This role involves the leading of several digital initiatives outlined in the Roadmap for which the Privacy and Information Security teams play an integral part in ensuring that these initiatives not only meet Ontario Health's obligations as set out in PHIPA but also general privacy and information security best practices. Key initiatives for the FY22/23 included a pilot to support collection of child and youth mental health data, as well as pilot initiative intended to streamline Drug & Alcohol Treatment Information System (**DATIS**) data submission for community mental health and addiction and facilitate a direct feed of this data into Ontario Health's Analytics Data Hub.

The Legal, Privacy and Information Security teams supported these initiatives by performing complex authorities analyses that involve intersecting pieces of legislation and complex contractual frameworks, informing the requirements for and development of new agreements, clarifying data flows, and conducting privacy and security assessments. While some assessment and agreements work is ongoing, the detailed reviews and assessments helped identify potential risks and barriers for the business unit which have informed project plans and strategic decision making for the MHA COE.

5. Privacy and Security by the Numbers: Key Metrics

The following key privacy and security metrics highlight some of the work accomplished by the Privacy Office and Information Security Office in 2022/23 and provides an indication of Ontario Health's compliance with legislative and regulatory requirements as well as with its privacy and security policies and procedures.

Highlights of Privacy Metrics

Ontario Health Privacy Breach Management

Ontario Health manages, or has custody or control of, a large volume of records and data sets. Ontario Health operates repositories and registries which contain data pertaining to individual encounters with the Ontario health care system and contains PHI, while the EHR portion of the data assets alone are more than 11 billion records that represent approximately 26.4 million unique individuals involving PHI. The metrics below include breaches of privacy policies and breaches where PHI was lost, stolen, or handled in an unauthorized manner. An example of a privacy breach is when an employee inadvertently accesses PHI where it is not required for the purposes of their job duties. Another example is when an external organization sends PHI to Ontario Health where Ontario Health did not request or need that information.

The volume of breaches is quite low in comparison to the volume of records, transactions, and potential for human error across the healthcare system and Ontario Health. All suspected and confirmed privacy breaches are investigated by the Privacy Office in collaboration with the relevant stakeholders, with mitigating strategies and recommendations implemented to prevent future breaches from occurring.

Privacy Breaches[5]				
	Apr-Jun 2022	**Jul-Sep 2022**	**Oct-Dec 2022**	**Jan-Mar 2023**
Breaches	32	37	31	31

Ontario Cancer Screening Program – Misdirected Correspondence

Over the 22/23 fiscal year, Ontario Health mailed over 7 million pieces of correspondence to individuals as part of the Ontario Health Cancer Screening Program, including for example, reminders to be screened and screening test results. These letters serve as a critical component of the Cancer Screening Program, which helps individuals detect cancer earlier when there is a better chance of treating it successfully, leading to better health outcomes.

In some instances, due to outdated or incorrect addresses from data sources, this mail is misdirected. Over the past fiscal year, 588 pieces of correspondence were delivered to an outdated or incorrect address and returned to Ontario Health as opened mail. Misdirected, opened correspondence represents 0.008% of the total volume of screening correspondence.

Each instance of returned mail is reviewed by the Ontario Health Cancer Screening Contact Centre who invalidates the incorrect address and attempts to update the intended recipients file with the correct address. Ontario Health will also send a breach notification letter to the intended recipient if the mail was misdirected and opened by an unintended recipient and if Ontario Health is able to update the address.

[5] Breaches caused by misdirected mail as part of the Cancer Screening Program are reported separately in this Report.

EHR Access & Correction Requests and Consent Directive Requests

Processing electronic health record (**EHR**) privacy requests related to access, correction and consent directives, support patients in exercising their privacy rights under the law. In Ontario Health's role as a prescribed organization in respect to the provincial EHR and in its capacity as an agent of health information custodians, Ontario Health:

- Receives and implements requests from patients to add, modify or revoke a consent directive on their records of PHI in the EHR; and
- Facilitates and assists contributing health information custodians with the administrative process related to individual access requests for records of PHI in the EHR, as well as to support the correction process where applicable.

EHR Privacy Requests				
	Apr-Jun 2022	**Jul-Sep 2022**	**Oct-Dec 2022**	**Jan-Mar 2023**
Access & Correction Requests	97	87	111	112
Consent Directive Requests	456	206	158	233

EHR Privacy Incident Management – Health Information Custodians and Coroners

Health information custodians and coroners are required to implement and adhere to their own internal privacy incident management policies for the management of privacy incidents in respect of PHI accessible by means of the EHR. Additionally, health information custodians and coroners who access or contribute records to the EHR must notify Ontario Health at the first reasonable opportunity upon identifying or becoming aware of a privacy breach related to PHI accessible by means of the EHR. Upon receiving this notification, Ontario Health reports the privacy breach to any other relevant health information custodians or coroner(s) that caused the breach or that contributed the record of PHI to the EHR. To further support the incident management process, Ontario Health provides EHR audit reports to health information custodians that enable them to audit and monitor their compliance with PHIPA.

HIC & Coroner EHR Privacy Breaches				
	Apr-Jun 2022	**Jul-Sep 2022**	**Oct-Dec 2022**	**Jan-Mar 2023**
Reported Privacy Breaches	8	8	15	19

Privacy Impact Assessments (PIAs)

A key function performed by the Privacy Office is the completion of PIAs that serve to assess a program or information system's privacy risks and recommend mitigating strategies. PIAs provide a level of assurance that privacy issues and risks are identified and resolved. They can also promote an understanding of how Ontario Health handles PHI or PI and demonstrate the ways in which Ontario Health meets its legislative and regulatory obligations and privacy commitment to the general public.

Privacy Impact Assessments				
	Apr-Jun 2022	**Jul-Sep 2022**	**Oct-Dec 2022**	**Jan-Mar 2023**
Completed PIAs	18	26	26	32

Highlights of Security Metrics

The below security key metrics highlight the number of completed internal and external Threat Risk Assessments **(TRA)**, other types of requested security assessments and penetration tests against new systems or changes to the operation. In addition, the table indicates the total number of internal and external events and incidents such as phishing attacks, or any kind of Indication of Compromise **(IOC)** that needed investigation. Also, to remain compliant with industry best practices and standards, the figures below detail the number of full vulnerability scans that were conducted across different network infrastructures within Ontario Health.

Key Cyber Security Activities - 2022-2023				
	TRA	**Security Assessment**	**Penetration Test**	**Incident Assessed**
Completed Number of Assessments by Type	64	80	16	42

6. Looking Forward

To continue delivering on its core mandate of integrating the health system and supporting superior patient-centered care, Ontario Health requires data – patient health information and personal information. The Privacy Office, Information Security Office and Cybersecurity teams have worked diligently over the last year to optimize the use of data and patient care while at the same time ensuring health data is managed in accordance with the agencies' legal obligations and commitment to protecting privacy and confidentiality. Through its prescribed roles Ontario Health has significant latitude to use data entrusted in its care and important responsibilities. As such, the work continues. Below is a sample of key priorities for the privacy and cyber security teams.

Enabling use of data across Ontario Health – Provincial Health Data and Digital Strategy (PHDDS) *(new)*

Ontario Health holds key health system data assets which were transferred from Ontario's legacy health system agencies pursuant to the *Connecting Care Act.* Ontario Health continues to acquire new data assets for system planning, and management, and at the request of the Ministry of Health for permitted purposes. Although these data assets continue to be managed in accordance with existing authorities and practices, the privacy, security and data acquisition and services team are working in lock step with Ministry of Health colleagues exploring, through further regulatory amendments and policy decisions, opportunities to broaden and/or streamline Ontario Health authorities to optimize the use of its data assets.

In the meantime, expanded use of these data assets across the organization requires implementation of privacy, security and information management practices and procedures that meet, at a minimum, the requirements of the Information and Privacy Commissioner with respect to Ontario Health's role as a prescribed entity and prescribed person. Over the coming year, the Privacy, Security and Data Acquisition teams will continue to support this work, which will progress in conjunction with the development of Ontario Health's Data and Analytics' strategy and the Ministry of Health's efforts on PHIPA modernization.

Bilateral discussions are underway between the Ministry of Health and Ontario Health to set near-term priorities for the development and implementation a proposed Provincial Health Data and Digital Service (**PHDDS**), including:

- Reviewing PHDDS background and policy direction
- Setting near-term work stream priorities and roles for:
    - Governance and policy
    - Operations and data management
    - Technology
    - Stakeholder/change management

Increasing Provider Access to Patient Health Records: Clinical consolidated viewer and EHR Clinical Data Foundations *(new)*

Ontario Health currently funds and supports three clinical viewers in Ontario that provide overlapping functionality to clinicians but currently serve different regions and continue to independently undergo releases, primarily driven by product roadmaps and end user feedback. Ontario Health is engaging in a program to consolidate these three clinical viewers to one standard provincial viewer for providers to access health information available in the EHR. This program consists not only of the establishment of the single provincial clinical viewer, integration with existing EHR repositories and registries, preparation for technical go-live, but also change management activities including planning and developing strategies for onboarding, training, communication, and preparation for pilots. In addition, and related to 'EHR access' above, to account for the 'digital means of access' requirements the scope of the Viewer Consolidation Strategy was expanded to also include a provincial patient viewer to provide individuals with a digital means of access to their EHR information.

At the same time the Acute and Community Clinical Data Repository (**acCDR**) is utilizing aging technology and is nearing end of life. This has resulted in functionality, technology, and data gaps for clinicians. Ontario Health will replace the existing acCDR to a new CDR on the new Clinical Data Foundations (**CDF**) common platform, including repository setup and configuration, terminology setup and configuration, data migration, data in/out setup, and data migration from acCDR to a new CDR. Other Ontario Health clinical data assets, including those that are part of the EHR, will also leverage the CDF and this project will be delivered over multiple phases and years.

Patients before Paperwork – Modernizing Provider Communication *(new)*

Ontario Health is supporting the Ministry of Health's efforts to reduce the use of fax and other paper forms in a health care setting that can be replaced with the use of digital means in an effort to place 'patients before paperwork'. As described below, this effort to digitalize health care communications will result in an increased ability to share patient records to support care and stronger security safeguards to protect patients privacy.

"According to the Ontario Information and Privacy Commissioner (**IPC**), misdirected faxes are the leading cause of unauthorized disclosure of personal health information in Ontario.

On September 21, 2022, a joint resolution on Securing Public Trust in Digital Healthcare was released by the federal, provincial, and territorial privacy commissioners. In this joint resolution the commissioners called on governments, health sector institutions and health providers to show concerted effort, leadership and resolve in implementing modern, secure, and interoperable digital health communication infrastructure.

This included a call for health care providers to phase out and replace traditional fax and unencrypted email systems for communicating personal health information with modern, secure, and interoperable systems "as soon as reasonably possible”.

On February 2, 2023, the Ministry of Health released its new health care plan, entitled *Your Health: A Plan for Connected and Convenient Care*. As part of the plan, the Ministry of Health committed to "axing the fax," and replacing antiquated fax machines with digital communication alternatives at all Ontario health care providers within the next five years.” [6]

Ontario Health is working with the Ministry of Health to develop and execute the five-year plan.

Medical Equipment Supplies (MES) *(new)*

The Privacy Office has been supporting the procurement efforts of the HCCSS’ in selecting vendors to support MES. As an extension of the MES modernization there will be corresponding enhancements made to CHRIS to make the system more efficient for HCCSS staff and clients, align changes to support new procurement contracts, provide HCCSS staff with better visibility into vendor performance, delivery, and inventory management, and provide patients and their caregivers, patient-centred, safe, timely, equitable, effective care. The enhancements will also include system integrations with the vendors. It is estimated that following successfully awarding contracts to vendors that there will be 12 PIAs required and corresponding privacy oversight over 2023/24 and 2024/25 to support assessment of vendors and the system integrations.

Digital eCorrespondance *(new)*

Ontario Health has launched an initiative to leverage and expand Ontario’s digital capabilities to modernize cancer screening communications and enhance the screening experience for Ontarians. The initiative seeks to align a digital correspondence solution with Ontario Health’s broader strategy for communicating with Ontarians about their healthcare. The Privacy Office has been engaged to provide support throughout the entire project lifecycle to ensure Privacy by Design principles are reflected in the solution design and delivery, and to ensure that risks are identified and remediated through collaboration with business partners and through a formal privacy risk assessment.

[6] https://www.lexology.com/library/detail.aspx?g=f179e4e0-c10a-499a-a818-e6fc7aee3557

Appendix A – Acronyms

Acronym	Meaning
acCDR	Acute and Community Clinical Data Repository
CBT	Cognitive Behavioural Therapy
CDF	Clinical Data Foundations
CHRIS	Client Health-Related Information System
CITIX	Cyber Threat Intelligence Sharing
COE	Centre Of Excellence
CPO	Chief Privacy Officer
CSD	Cyber Security Defense
CSF	Cyber Security Framework
CSOM	Cyber Security Operating Model
DATIS	Drug & Alcohol Treatment Information System
DHDR	Digital Health Drug Repository
DHIEX	Digital Health Information Exchange
EHR	Electronic Health Record
ESP	Electronic Service Provider
FIPPA	*Freedom Of Information And Protection Of Privacy Act*
FOI	Freedom Of Information
HCCSS	Home And Community Care Support Services
HCNS	Health Care Navigation Service

Acronym	Meaning
HCO	Health Connect Ontario
HIC	Health Information Custodian
HINP	Health Information Network Provider
HPV	Human Papillomavirus
HSPS	Health System And Performance And Support
IOC	Indication Of Compromise
IPC	Office Of The Information And Privacy Commissioner Of Ontario
IRN	Response Notification
ISO	Information Security Office
ISSC	Information Security Steering Committee
LDG	Local Delivery Group
MES	Medical Equipment Supplies
MHA	Mental Health & Addictions
MSSP	Managed Security Service Provider
NIST	National Institute Of Standards And Technology
NLO	Network Lead Organization
NPWT	Negative Pressure Wound Therapy
NT OHT	North Toronto Ontario Health Team
O. Reg.	Ontario Regulation
OCC	Ontario Case Costing

Acronym	Meaning
OCSR	Ontario Cancer Screening Registry
OHDC	Ontario Health Data Council
OLIS	Ontario Laboratories Information System
ORN	Ontario Renal Network
PE	Prescribed Entity
PHDSS	Provincial Health Data and Digital Service
PHI	Personal Health Information
PHIPA	*Personal Health Information And Protection Act*
PI	Personal Information
PIA	Privacy Impact Assessment
PO	Prescribed Organization
PP	Prescribed Person
RSOC	Regional Security Operation Centres
SIEM	Security Information And Event Management
SOC	Security Operating Centre
TGLN	Trillium Gift Of Life Network
TRA	Threat Risk Assessment
WTIS	Wait Times Information System
XDR	Extended Detection And Response