2024 / 2025 Ontario Health Annual Privacy and Security Report

May 2025

Ontario Health

Table of Contents

Introduction

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 Protection Act* (**PHIPA**), the *Freedom of Information and Protection of Privacy Act* (**FIPPA**), and the *Gift of Life Act* 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.

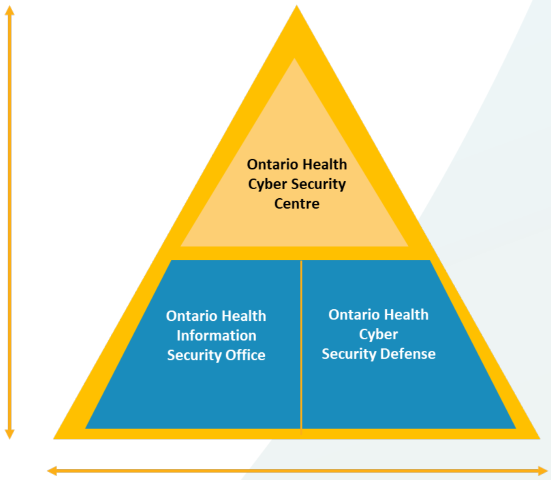
In 2024/25 Ontario Health's Privacy and Information Security teams in collaboration with other business partners across Ontario Health and the province, have continued to work together to remove barriers and address new PHIPA authorities, data privacy, cyber security, interoperability, and other compliance 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 2024/25 fiscal year that support and advance Ontario Health in achieving its mandate. The report also looks back at key metrics, some of which are reported to the Office of the Information and Privacy Commissioner of Ontario (**IPC**) and looks forward to privacy and security priorities for 2025/26.

Background

Ontario Health Cyber Security Program

The Ontario Health Cyber Security Program is a collaborative partnership comprised of three specialized teams: the Ontario Health Cyber Security Center, the Information Security Office and Cyber Security Defense. Together, these teams facilitate, strengthen, and sustain the information and cyber security posture of Ontario Health and the provincial health care sector. The program aims to protect information and system assets, ensuring alignment with business objectives and industry standards, while strengthening access to care for patients and providers.

Cyber Security Governance and Partnership


Ontario Health Cyber Security Centre
Ontario Health Information Security Office
Ontario Health Cyber Security Defense

The **Ontario Health Cyber Security Centre** (**OHCSC**) provides direction, leadership and governance in cyber security for the province's health care system. The centre supports a vision for the management of cyber security risk across the provincial health sector and is predicated on supporting the delivery of cyber security capabilities at the provincial, regional and health service provider levels. The centre works closely and collaboratively with the Ontario Health Information Security Office and Ontario Health Cyber Security Defence team to deliver a collective approach to safeguarding Ontario Health digital assets.

Through the creation of a risk-based security program within the Digital Excellence in Health portfolio, the **Ontario Health Information Security Office** (**ISO**) has designed physical, technical and administrative safeguards to ensure a safe and secure environment for the delivery of digital health care solutions. These safeguards are implemented in accordance with legislative requirements, international standards and prioritized risk-based decisions to ensure confidentiality, integrity and availability of data and services.

The Information Security Office is accountable for Security Architecture, Security Governance, Risk and Compliance, Third Party Security Risk Management, Threat Risk Assessments and Security Awareness and Training. The team provides services for the identification, assessment and mitigation of security risks; internal security advisory services; and supporting the response to incidents and breaches in conjunction with the **Cyber Security Defense** (**CSD**) team.

The CSD team is responsible for the front-line defense and management of the technical components of security at Ontario Health. This group includes Security Operations Center (**SOC**), Vulnerability Management, Identity and Access Management (**IAM**), Incident Response, and Security Platform Engineering. CSD manages and prioritizes a variety of ongoing initiatives based on both the internal risk of the item, and the continuously evolving external threat landscape.

At Ontario Health, in alignment with its Privacy Program, security is a core design principle embedded across all systems and digital operations. Through a "security by design" approach, we integrate security considerations throughout the development lifecycle and operations, proactively identifying and mitigating risks to protect sensitive information and defend against cyber threats.

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 and change. 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, the IPC as well as its key provincial stakeholders and partners in order to fulfill its mandate.

The Privacy Office, with its Information Security partners, and other business partners, has the responsibility to:

- Maintain public trust and protect individual privacy and the confidentiality, security, and availability of billions of data assets;
- Enable our business partners to receive, collect and use these data assets in alignment with applicable privacy laws and in support of Ontario Health's mandate to optimize patient centered-care;
- Obtain IPC approval of Ontario Health's policies and procedures every 3 years in order to continue delivering on Ontario Health's mandate; and
- Remove barriers and advocate for changes required to transform the health data ecosystem.

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 Strategy, Planning, Privacy, Analytics and Risk portfolio whose mission is to strive to meet and exceed the needs of Ontario Health while improving on tools, methodologies, and processes. The privacy program is led by the Chief Privacy Officer (**CPO**), who reports directly to the Chief, Strategy, Planning, Privacy, Analytics & Risk. A team of dedicated privacy professionals, managers and a director support the CPO in upholding public trust by managing the day-to-day operations of Ontario Health's privacy program, which includes:

- collaborating with the Ministry of Health, the IPC, and other provincial stakeholders on the establishment of new authorities that will allow Ontario Health to deliver new services and programs to Ontarians,
- identifying opportunities to streamline existing authorities and practices, mitigating risks for Ontario Health by designing user centric privacy business requirements for new programs, services and technologies;
- evaluating vendor proposals and helping support vendor management,
- supporting new data acquisitions and uses, leading policy development initiatives;
- overseeing the content development and deployment of mandatory and just in time privacy training,
- managing the suite of privacy operational obligations which include applying individual consent directives, privacy breach investigation and management, working with health care providers across Ontario to respond to access, and correction requests.

In partnership with information security and other business partners across all portfolios, the Privacy Office not only provides operational, advisory and assurance services but also risk-based, pragmatic, and creative privacy solutions that 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, disclose and otherwise handle 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 to deliver on its mandate, for its operations and to optimize its permitted use of data for good.

Prescribed Entity (PE)

Ontario Health is designated as a 'prescribed entity' for the purposes of subsection 45(1) of 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 registry of cardiac and vascular services (managed by legacy CorHealth). 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)

Ontario Health is designated as a 'prescribed organization' for the purposes of Part V.1 of PHIPA. This designation grants Ontario Health the authority to develop and maintain the electronic health record (**EHR**), building 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.

The EHR is comprised of the provincial client and provider registries, laboratory, prescription drug, diagnostic imaging (common services), and clinical documents repositories, where records are received from health information custodians such as hospitals and family health teams. As a prescribed organization, Ontario Health enables access to PHI held in the EHR for authorized health care providers for the provision of healthcare, 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.

In the near future, Ontario Health will be authorized to provide Ontarians with a digital means to access their PHI held in the EHR.

PHIPA Agent

The definition of agent in PHIPA includes any person (including organizations, 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. For example, as a PHIPA Agent, Ontario Health is authorized to manage components of the Health811 (**H811**) program on behalf of the Ministry of Health, who is the custodian.

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 PI. Ontario Health's collection of PI 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 PI , including PHI , for the purposes of planning, coordinating, supporting, researching, and reporting on all aspects of organ and tissue donation and transplantation. This handling of PI 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 PI 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.

Individual Access to the Electronic Health Record (EHR) (new)

In July and December 2024, changes to Ontario Regulation 329/04 and PHIPA respectively, were proposed to enable Ontario Health, as a prescribed organization, to provide individuals with digital access to their records of PHI held in the EHR, beginning with laboratory, medication, and pharmacy service records. This digital access will rely on the identity proofing service described below. Ontario Health continues to collaborate with the Ministry of Health with respect to these proposed changes, which are not yet in force.

Digital Health Identifier (DHI) (new)

In July and December 2024, changes to Ontario Regulation 329/04 and PHIPA respectively, were proposed to enable Ontario Health, under a new PHIPA authority, to provide individuals with a digital means to validate and verify their identity, for the purpose of connecting with digital health tools offered by Ontario Health and other health care organizations across the province. This identity proofing service will support individual access to the EHR as described above. Ontario Health continues to collaborate with the Ministry of Health with respect to these proposed changes, which are not yet in force.

Mandatory Contribution to the EHR (new)

On January 01, 2025, changes to Ontario Regulation 329/04 under PHIPA came into force which mandate contribution to the EHR from certain priority sectors to ensure more complete patient records. More specifically, in addition to the existing requirement for operators of public hospitals, operators of accredited community pharmacies and integrated community health services centres are now also required to contribute certain PHI to the EHR as requested by Ontario Health and in accordance with Ontario Health's interoperability specifications.

Bill 194: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024 (new)

Bill 194 was introduced in May of 2024 with two schedules. Schedule 1 introduced new legislation, the *Enhancing Digital Security and Trust Act, 2024* (**EDSTA**), aimed at enhancing cyber security within the public sector. Schedule 2 amends the *Freedom of Information and Protection of Privacy Act* (**FIPPA**) to enhance and modernize privacy protections. The EDSTA applies across the provincial and municipal public sectors, and gives the government the ability to enact regulations that require public sector entities to:

- Have cybersecurity programs that include elements relating to the assignment of internal responsibility, education awareness, incident response and program oversight; and
- Submit cyber security incident reports and set requirements for such reports.

The EDSTA also gives the Minister of Public and Business Service Delivery the ability to establish technical standards and issue cyber security directives.

EDSTA introduces artificial intelligence (AI) obligations for public sector organizations, such as Ontario Health, including:

- Publishing information about their use;
- Developing and implementing an accountability framework;
- Managing risks associated with the use of an AI system; and
- Appointing an individual to oversee the use of AI systems and meet other stipulated obligations.

Finally, EDSTA gives the government the power to enact regulation governing the processing of minors' information by children's aid societies and school boards.

FIPPA Changes

Ontario Health is an "institution" under FIPPA with respect to its handling of PI. Bill 194 introduces new breach reporting and privacy impact assessment requirements for FIPPA institutions. It also expands the powers of the IPC to investigate privacy compliance, granting the IPC new order making powers.

Changes in privacy breach reporting for breaches involving PI and notification include the following:

- Bill 194 uses the "real risk of significant harm" (RROSH) threshold for breach reporting and notification. Ontario Health will be required to report to the IPC and notify affected individuals if there is reason to believe there is a RROSH associated with a breach of PI.
- Ontario Health will be required to keep a record of every theft, loss, and unauthorized use or disclosure of PI that it reports the IPC.
- Ontario Health will be required to submit an annual report to the IPC that summarizes the number of thefts, losses, and unauthorized uses or disclosures of PI.
- Ontario Health will be required to conduct privacy impact assessments (**PIAs**) with specific content requirements before collecting PI and to update PIAs where a change to PI handling is expected.
- Ontario Health, when acting as an "institution" under FIPPA, is required to implement reasonable safeguards to protect PI from theft, loss, and unauthorized use or disclosure, and to protect against unauthorized copying, modification, or disposal.
- Bill 194 will expand the IPC's privacy compliance investigation powers giving the IPC the power to conduct complaint-based and proactive reviews of an institution's information practices.
- Finally, Bill 194 will provide for confidential "whistleblower" reports to be made directly to the IPC, barring the IPC from revealing the identity of the person who made the report.

As of July 01, 2025, both the EDSTA and all FIPPA changes introduced in Bill 194 will have come into force.

Key Privacy and Security Milestones and Achievements

In 2024/25, the privacy and security teams focused on achieving the following goals.

Ontario Health Data Council (OHDC) (updated)

In 2024/25, the Privacy Office, in collaboration with the Digital Excellence in Health and the CorHealth team, submitted the first request to the EHR Advisory Working Group and subsequently to the Ontario Health Data Council (**OHDC**), for the Minister to direct Ontario Health as a prescribed organization to disclose PHI held in the EHR, to Ontario Health as prescribed person, to facilitate or improve the provision of cardiac care through the Data Collection Information System (**DCIS**). This request was approved in January of 2025.

The DCIS is a modern analytics service in support of CorHealth Cardiac Centres surgical procedure efficiencies.

The DCIS collects surgical wait times related data from the 20 Cardiac Centres participating in the cardiac and vascular services CorHealth network. The limited EHR data, when queried, will ensure cardiac records are as accurate as possible.

Established in 2021, the 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's Chief of Strategy, Planning, Privacy & Analytics participates as a member of the OHDC advises 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 (1) of PHIPA.

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." [1]

EHR Advisory Support Working Group (updated)

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[2]:

"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 PHI 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 PHI 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 PHI 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 PHI 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 PHI 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

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

Privacy Training and Awareness – Privacy Day (updated)

January 27 to 31, 2025, was Data Privacy Week, an extension of Data Privacy Day

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

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

(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 January 28, the IPC hosted a Privacy Day Event: Key issues discussed included the latest developments in privacy enhancing technologies and how they allow organizations to make use of data without compromising privacy.

To further increase privacy awareness among Ontario Health employees, the privacy team, deployed a month-long campaign of providing key privacy messages on computer lock screens to help re-enforce learning, published a series of weekly newsletters throughout the month of January on various themes and introduced a net-new blog article featuring Ontario Health's Chief Privacy Officer. Examples of the weekly newsletter themes included:

- Your 2025 Resolution: Improve Your Data Privacy Literacy
- Protecting Privacy at Work and Beyond
- Deceptive Design Patterns and Your Privacy
- Digital Literacy & Privacy: Empowering Ontario's Seniors and Youth in a Digital Age
- Embracing AI with Privacy in Mind
- Vantage Point Blog: Sharing Versus Over-Sharing

Ontario Health's Review and Approval by the Information and Privacy Commissioner (IPC) (updated)

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.

Approval from the IPC allows Ontario Health to continue delivering on its mandate, which includes health system planning, cancer screening, research, wait time information management, and the development and maintenance of the provincial EHR.

Throughout 2024/45, Ontario Health has been working diligently in preparing for the 2026 triennial review by the IPC. On August 1, 2025, Ontario Health will submit Privacy, Information Security, Human Resources, and Organizational indicators to the IPC.

The IPC will review the submitted indicators, request additional documentation and information, where needed, and determine which policies, procedures, and practices will be the focus of this IPC triennial review.

The policies, procedures, and practices will be assessed to ensure that they protect the PHI received by Ontario Health under its prescribed statuses, and whether Ontario Health is adhering to these policies, procedures, and practices.

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

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, information 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 IPC with respect to Ontario Health's role as a prescribed entity and prescribed person. Over the coming year, the privacy, information 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 proposed Provincial Health Data and Digital Services (**PHDDS**), including:

- Recommending policy directions to support a 'Collect Once Use Many' approach to the use of data and streamlining Ontario Health privacy authorities.
- Identifying requirements to support policy recommendations and assessing impact of proposed policy changes.
- Working with the Ministry of Health to amend PHIPA to expand OH registries into a Registry of Chronic Disease that will enable the establishment of the Ontario Abdominal Aortic Aneurysm Program and quality improvement planning.

In line with recommendations outlined by the OHDC, the current PHDDS strategic project is focused on exploring options that will enable Ontario Health's ability to "Collect Data Once, Use Many Times", supported by unifying and advancing data governance practices through establishing data governance and stewardship framework, harmonizing standards and modernizing existing data and digital infrastructure.

Maturing the Privacy Incident Management Process (new)

During 2024/25, the Privacy Office continued to mature Ontario Health's Privacy Incident management process by:

- Leading the revision of the *Privacy Incident Management Policy and Procedure* and the *EHR Privacy Incident Management Policy and Procedure* to clarify the processes which Ontario Health Agents must follow when managing privacy incidents.
- Providing privacy incident management education sessions to Ontario Health employees.

Hosting the first privacy-specific incident investigation tabletop exercise. Tabletop exercises provide insight into the privacy incident response process, clarify roles and responsibilities, and identify gaps, with the goal of improving awareness of the privacy incident management process. This successful exercise included participation from Ontario Health staff from the Privacy Office, Communications, Cyber Defence, Human Resources and Legal.

Privacy Optimization Project (new)

The privacy team identified opportunities to streamline a number of privacy program activities including optimizing intake processes, exploring leveraging tools and technology, establishing project prioritization processes with its many business partners and setting the foundation for an enhanced framework for managing privacy risks and controls through a 'Three Lines of Defense' (**3LOD**) model. Implementing these enhancements, will create opportunities to increase operational efficiency, reduce manual workload, and enable business units to take a more proactive role in day-to-day management, including mitigation of operational risks, This work will extend to the end of fiscal 2025-26.

Advancing Sector-Wide Cyber Capabilities: Ontario Health Cyber Security Centre (update)

In 2024/25, the Ontario Health Cyber Security Centre (**OHCSC**) focused its efforts on progressing the operationalization and strategy of the Provincial Cyber Security Operating Model (**CSOM**).

These steps included:

- Evolving best practices by transitioning to the National Institute of Standards and Technology (**NIST**) Cybersecurity Framework 2.0;
- Developing and operationalizing an initial critical controls tracker to measure progress and maturity of prioritized critical controls by acute Health Service Providers (**HSPs**);
- Enhancing threat intelligence and monitoring by launching a Cyber Threat Intelligence Exchange (**CTIX**) platform;
- Testing readiness and established incident response processes through participation in two tabletop exercises (**TTX**) with Ministry and sector partners;
- Identifying and prioritizing the protection of valuable assets through the initial development of a crown jewels asset repository;
- Engaging with HSPs beyond the scope of acute care entities to better understand and strategize how these providers can be integrated within the CSOM's next iteration; and
- Advancing and building out capabilities, content and resources on the dedicated cyber health portal for the sector.

The CSOM consistently demonstrates its effectiveness in enhancing the availability and resilience of patient care, laying the groundwork for its ongoing development and enhancement. Patients and communities throughout the province will continue to benefit from a health care system that safeguards patient services and data, leading to improved health outcomes. The upcoming phase of the CSOM promotes a more cooperative approach to cyber security, driving sector-wide advancements to protect patient care and information while strengthening defenses against emerging cyber threats.

Harmonizing Cyber Security Standards (new)

During the 2024/25 fiscal year, in collaboration with the Architecture Program, Network Services and Cloud Operations teams, the following security architecture standards were implemented:

- **Zero Trust Architecture Standard**: This approach provides reference architecture for a risk-based cyber security strategy. The communication between users, systems, and devices is continuously authenticated, authorized, and validated. A Zero Trust architecture enforces access policies based on context such as the user's role, the time of day, geolocation, the device, and the data they are requesting. The level of access granted is dynamically adjusted based on the level of trust established with the subject. In short, the more trust that an information system can develop in a subject, the more access that subject can be granted.
- **Network Security Zone Standard**: Security Zoning is a key part of the defense-in-depth strategy to protect Ontario Health's networks and support electronic service delivery, interconnectivity and interoperability. The standard defines security zoning and high-level communication flows which are permitted between zones so that departments and squads in Ontario Health can enhance their security posture. The guidance in this standard is applicable to both on-premises and cloud environments.

- **Amazon AWS Cloud Security Architecture Standard:** This standard defines a reference architecture to ensure a secure implementation and deployment of products and services to Ontario Health's AWS tenant.
- **DevSecOps Standard:** This standard provides the guiding framework for integrating security into the DevOps process, ensuring that security considerations are embedded throughout the software development lifecycle.
- **Dynamic Application Security Scanner Tool (DAST)**: This security testing mechanism was introduced in the cloud Azure product subscriptions to integrate security testing early into the product development lifecycle. DAST is also being provisioned to Ontario Health on-premise environments (**OHDC**) and is targeted to commence security testing.

Third-Party Risk: Building Resilience Beyond Ontario Health Walls (new)

Threat actors are increasingly targeting technology and service providers because compromising a trusted third-party supplier can be an effective way to gain access to many organizations and downstream suppliers. Accordingly, Ontario Health's existing policies and practices to manage third-party security risks are evolving to handle the rise and complexity of its supplier relationships and health care sector partnerships.

Ontario Health's Information Security Office (**ISO**) has undertaken enhancements of the Third-Party Security Risk Management (**TPSRM**) program in alignment with industry recommendations for maturing TPSRM capabilities. Improving integration of TPSRM functions within business lines ensures better process integration with key enterprise functions such as procurement, project governance, business delivery and enterprise risk management. Robust third-party security risk monitoring and dashboard reporting throughout the third-party relationship provides continuous visibility into third-party security risks and facilitates effective senior management engagement and risk decisions. Constructively leveraging industry certifications (e.g., ISO/IEC 27001, HITRUST r2), control attestations (e.g., SOC 2) and third-party audits as they were intended to serve, helps streamline and standardize how third-party security risks are evaluated and enables security resource optimization. With stakeholder consultation, the ISO established and formalized the *Third-Party Security Risk Management Standard* and the *Third-Party Security Risk Management Framework* in fiscal year 2024-2025 and the *Framework* will be operationalized within fiscal year 2025-2026.

Maturity Matters: Understanding Our Security Readiness (new)

As part of Ontario Health's ongoing commitment to strengthening its cyber resilience, the Ontario Health Cyber Security Teams launched an internal Cyber Security Maturity Assessment initiative. This assessment leverages the Axio360 platform, aligned with the newly updated NIST Cybersecurity Framework (**CSF**) 2.0, and tailored with the Ontario Health Cyber Security Centre.

The purpose of this initiative is to systematically evaluate Ontario Health's current cyber security posture, identify areas of strength, uncover opportunities for improvement, and prioritize targeted enhancements. This proactive assessment supports alignment with the provincial cyber security standards and reinforces our organization's role within a broader, integrated health system security model.

This initiative began in Q4 of FY 2024-2025, in collaboration with internal partners across multiple business units, and is expected to provide strategic insights that will directly inform cyber security planning, resourcing and goal setting for FY25/26. The assessment will also serve as a foundational step toward continuous improvement, helping ensure that Ontario Health is well-positioned to manage evolving threats and protect the sensitive data entrusted to us and maintain public trust.

Boosting Information Security Collaboration Across Ontario Health (updated)

Ontario Health cyber security teams continue to strengthen its collaborative approach through the evolution of the Information Security Knowledge Exchange **(ISKE**). Launched as a strategic enhancement to the former Information Security Steering Committee (**ISSC**), ISKE was developed to better address the evolving needs of cross-functional teams by fostering a more proactive and integrated approach to information security across the organization.

Held bi-monthly, ISKE meetings bring together partners from cyber security, privacy, product, compliance, architecture and operations. Sessions include spotlight presentations, key updates, and in the future, external guest speakers who provide insights on trends, risks and best practices. Topics have included cyber security threats, regulatory compliance, data privacy, cloud and network security and incident response strategies.

Each session is designed to go beyond routine updates, using spotlight presentations to highlight timely and relevant topics such as cyber security trends, IPC reporting and regulatory compliance, data privacy, incident response strategies, cloud and network security, and access management. The meetings include diverse formats—ranging from presentations, panel discussions to case studies and Q&A sessions—to maximize engagement and encourage open dialogue across disciplines.

ISKE promotes open knowledge sharing, supports alignment between technical and business teams, and helps cultivate a strong culture of cyber security awareness, accountability, and resilience in the face of evolving cyber risks.

Amplifying Security Awareness Training (updated)

Ontario Health procured the Canadian Internet Registration Authority (**CIRA**) cyber security awareness and training platform to support regular and annual role-based cyber security awareness training, adaptive phishing simulations, and inform plans to improve Ontario Health's cyber risk profile. Ontario Health adopted the CIRA solution to enhance its cyber security infrastructure and protect its digital assets and operations. This solution enables Ontario Health to build resiliency within its workforce to safeguard sensitive information and mitigate cyber threats.

During the fiscal year 2024-2025, Ontario Health successfully completed several critical initiatives under the CIRA solution:

- **Deployment of Advanced Security Protocols:** Ontario Health integrated cutting-edge security protocols, including DNS-based threat protection and automated incident response mechanisms, which have significantly reduced the risk of cyber-attacks.
- **Training and Awareness Programs:** Comprehensive training sessions were conducted to educate staff about best practices in cyber security and the usage of CIRA tool, enhancing the overall security posture of the organization.
- **Regular Security Audits:** Routine security audits were performed to identify vulnerabilities and ensure compliance with

national and international cyber security standards.

- **Collaboration with CIRA:** Continuous collaboration with CIRA experts facilitated the timely deployment of updates and the optimization of security measures tailored to Ontario Health's specific needs.
- **Phishing Campaigns**: Ontario Health conducts monthly phishing simulation campaigns to assess staff awareness. Over the last year, we reduced phishing incidents with training programs and enhanced security measures, including advanced threat detection systems.

Awareness to Action: Increasing Security Education and Literacy (updated)

To keep pace with and better defend against a variety of cyber incidents and attacks, a new and revamped means of educating Ontario Health team members was required.

The Information Security Office (**ISO**) with a support from Cyber Security Centre and Cyber Security Defense teams employed the following programs to develop a more robust security culture environment:

Internal Communication:

- Posted regular and timely security articles to the Ontario Health Pulse (e.g., internal intranet page) to reinforce key messages.
- Conducted regular Lunch & Learn sessions with Ontario Health team members on relevant topics and real-time events to help boost knowledge.

Dynamic Feedback Loop:

- Monitored new attack techniques by collaborating with Managed Security Service Provider (**MSSP**) and directly funneling them into awareness campaigns within days of observance.
- Additional tactics and techniques employed by attackers are facilitated through the training cycle to boost knowledge for team members.

Enhancing Annual Security Awareness Training

- Revitalized the annual training module to incorporate new technology, domains and relevant topics to impart enhanced learning.
- Conducted a gamification roll out and security challenge competition as part of a broader cyber awareness campaign.
- Conducted fire side chat with security leaders and pathways to cyber security sessions to help educate team members about cyber security career paths.

Engaging Learning and Development

- Conducting a needs-based analysis in partnership with Ontario Health's Learning and Development team to determine what areas of the current cyber awareness program could be enhanced and improved.

Cyber Security Awareness Month

During the month of October, interactive sessions and engaging intranet articles played a central role in fostering community-wide engagement. The month was also enhanced by creative engagement strategies, such as themed lock screen messages and Microsoft Teams' meeting backgrounds designed to keep cyber security prominently in the minds of our team members. Through these varied educational and experiential approaches, the program took steps to further foster a proactive and well-informed organizational culture adept at managing ongoing cyber security challenges.

Modernizing Digital Identities, Enhancing Data Governance and Boosting Threat Management and Response (new)

Hybrid Security Operations Centre Monitoring and Response
During fiscal year 2024-2025, the 24/7 Hybrid Security Operations Center (**SOC**) at Ontario Health conducted extensive monitoring and response activities. This critical function ensured the detection and mitigation of threats in real-time, maintaining the integrity and security of our systems across the organization. These efforts were pivotal in strengthening our cyber defense mechanisms and reducing the impact of potential cyber threats. This initiative reflects our commitment to adapting to the rapidly evolving cyber threat landscape and maintaining a high level of security and compliance.

Product-Focused Vulnerability Management
In response to the evolving threat landscape, Ontario Health implemented a new product-focused strategy aimed at better prioritizing and mitigating vulnerabilities. This approach expands the scope of vulnerability management to include both application and configuration vulnerabilities, improving accountability, visibility and mitigation efforts for each product group. This strategy has enabled more targeted and effective vulnerability management, ensuring that compensating controls are implemented, bolstering the overall security posture of our products and supporting the organization's objectives.

Protection for EDR Ineligible Operating Systems (OS)
In fiscal year 2024-2025, the SOC addressed the challenge of protecting operating systems (**OS**) that are ineligible for industry-leading Endpoint Detection & Response (**EDR**) solutions. Conducting thorough research, proof of value (**POV**) and procurement, Ontario Health identified a solution that provides security protection comparable to EDR for these systems. The project has commenced with implementation underway for a targeted set of systems, ensuring that these systems are safeguarded against potential security threats. This proactive approach mitigates the risks associated with these systems and enhances the protection of our digital assets, reflecting our innovative approach to cyber security.

Enterprise Identity and Access Management Program
The Enterprise Identity and Access Management (**EIAM**) Program is a strategic initiative designed to modernize and secure Ontario Health's management of digital identities and access. At its core, EIAM provides a centralized and scalable identity framework that ensures individuals receive the right access to the right resources at the right time—and for the right reasons. The program leverages advanced technologies including Multi-Factor Authentication (**MFA**), Single Sign-On (**SSO**), and Role-Based Access Control (**RBAC**) to enforce strong security controls. These capabilities protect sensitive data, reduce insider threat exposure and support compliance with regulatory standards.

In 2024-2025, the program achieved several significant milestones:

- Successfully procured and implemented the Saviynt platform, integrating Identity Governance and Administration (**IGA**) and Cloud Privileged Access Management (**CPAM**) capabilities
- Completed foundational configurations, including integrations with Ontario Health Cloud AD, Entra ID and Workday
- Converged business processes between legacy and cloud-based directories and migrated on-premises CyberArk PAM solution to the CyberArk Privilege Cloud Software as a Service (**SaaS**) platform,

marking a major shift toward modern, scalable and AI-driven identity services.

Following these changes, the program has delivered significant business value. In particular, the program has significantly reduced on-premise, eliminated disruptive downtime for patching cycles and reducing overtime. The move to cloud has also optimized resource allocation, lowered the total cost of ownership, and positioned the organization to decommission legacy tools.

Zero Touch Certificates and Key Management Program

The Zero Touch Certificates and Key Management Program (**ZTKMP**) is a modernized approach to managing digital certificates and encryption keys with minimal human intervention. This program aims to enhance the security and efficiency of cryptographic operations across the organization. ZTKMP seeks to automate the lifecycle management of certificates and keys, from issuance and renewal to revocation and storage, leveraging modern technologies such as blockchain and artificial intelligence.

In 2024-2025, ZTKMP addressed the global distrust of Entrust’s root certificates by using a semi-automated process to replace the old certificates with newly procured certificates. As part of this modernization effort, the team developed and launched an RFP for the broader ZTKMP initiative, laying the foundation for a fully automated, AI-driven certificate lifecycle management platform. In parallel, the Public Key Infrastructure (**PKI**) team successfully issued or renewed over 5,000 certificates (public and private), reinforcing digital trust and operational resilience across the enterprise.

Cyber Security Incident Response Management Program

The Cyber Security Incident Response Management Program (**CSIR-MP**) is dedicated to preparing for, responding to, and recovering from cyber security incidents. This program plays a crucial role in maintaining the resilience and integrity of the organization's digital operations.

In an era where cyber threats are increasingly sophisticated and pervasive, the ability to swiftly and effectively manage incidents is paramount. CSIR-MP encompasses a comprehensive set of procedures and tools designed to detect, analyze, and mitigate the impact of cyber security incidents. This includes the establishment of an incident response team, the deployment of advanced monitoring systems, and the creation of detailed incident response plans.

CSIR-MP has significantly enhanced the organization's ability to respond to and recover from cyber incidents, minimizing downtime and mitigating damage. The program has fostered a culture of vigilance and preparedness, ensuring that employees are well-equipped to recognize and report potential threats. Through regular training and simulations, the organization has built a robust incident response capability that can swiftly counteract and contain threats.

Previewing Microsoft Purview

The Microsoft Purview Tool is a comprehensive solution designed to enhance data governance and information protection across Ontario Health. This tool was introduced to address the growing need for robust data security measures in the era of artificial intelligence (**AI**). Microsoft Purview provides integrated coverage to manage and protect sensitive data throughout its lifecycle, wherever it resides. The tool includes features such as data loss prevention, data security posture management, information barriers, information protection, insider risk management and privileged access management.

The implementation of Microsoft Purview aligns with Ontario Health's Information Classification and Handling Standards, ensuring that data is appropriately labeled and protected. The deployment of Microsoft Purview began with a proof of concept involving approximately 70 individuals. This initial phase introduced data labels aligned with Ontario Health's standards and demonstrated the tool's effectiveness in safeguarding sensitive information. The project is spearheaded by the Security Platform Engineering team.

The benefits of Microsoft Purview include enhanced visibility into data across the organization, improved data security and compliance with regulatory requirements.

Securing Remote Access Through Netskope (new)

Netskope solution is a remote access tool designed to enhance secure internet and private access for Ontario Health. It was selected as the primary corporate Secure Service Edge (**SSE**) tool to replace Zscaler, which had been used in a proof of concept with approximately 3,000 users, as it offered a more cost-effective and integrated solution with comprehensive security features. Netskope provides secure internet and private access, integrates seamlessly with existing security tools, and marks a significant milestone in the organization's journey towards a Zero Trust security model.

The phased rollout of Netskope began in mid-February and was completed by March 31, 2025. This deployment involved remote installation on users' devices, ensuring minimal disruption to their workflow.

Key Program and Project Initiatives

The Privacy Office in collaboration with the Information Security Office 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.

Provincial Patient Viewer – Enabling Individuals to Access to their records of PHI held in the EHR (updated)

In the past, individuals have been able to directly access some of their health records via patient portals (e.g., MyChart, myUHN) which are not developed or maintained by Ontario Health.

The provincial EHR is developed and maintained by Ontario Health as a prescribed organization. Providing individuals with digital access to their PHI held in the provincial EHR, is critical to enable better care. Ontario Health is developing a Provincial Patient Viewer which would allow Ontario Health to provide individuals with direct and digital access to their records held in the EHR. While legislative and regulatory changes which would permit Ontario Health to make the viewer available are not yet in force, it is anticipated that Ontario Health, under its role as a prescribed organization, will act as if it had custody or control of the records to provide an individual with access to Ontario Laboratories Information System (**OLIS**) and Digital Health Drug Repository (**DHDR**) records to start, and later Diagnostic Imaging-Common Service (**DI-CS**) and Acute and Community Clinical Data Repository (**acCDR**) records.

Ontario Health continues to work with the Ministry of Health to ensure that this program will best support individuals in digitally accessing their records held in the EHR, while simultaneously protecting these highly sensitive records of PHI. Over the course of the last year, the Ministry of Health and Ontario Health have continued to collaborate on a framework that can support Ontario Health with its journey to meet the privacy, security, technological, procedural, and programmatic requirements to enable this program to launch. This program is also aligned with the "Digital Access for Patients" pillar of the Ministry's Digital First for Health strategy.

Digital Health Identity – Enabling Individuals to validate and verify their identity to connect with digital health tools (updated)

Where individuals seek to access PHI, they are required to verify their identity, to help ensure that this highly sensitive information is only shared where appropriate.

Ontario Health is implementing a provincial Digital Health Identity (Patient Access) Program, leveraging the components of an existing solution, integrated with common government enterprise services from the Ministry of Public and Business Service Delivery and Procurement (**MPBSDP**), to deliver the people of Ontario with a trusted and secure digital identity that can be used to access digital health care services and information.

Key objectives include:

- Enabling a secure, trusted and provincially scaled patient identity and access management solution.
- Integrating this solution with the Provincial Patient Viewer as a priority digital health service.
- Providing a secure, standards-base, and efficient way to onboard additional digital health services in the future e.g. Health811, Digital Correspondence.

Ontario Health privacy and legal team members have provided detailed recommendations to the Ministry to inform a legal framework that would give Ontario Health a new role and legal authority under PHIPA to oversee this digital identity program for the province.

Canada's federal, provincial, and territorial privacy regulators (including Ontario) issued a joint resolution calling on governments and stakeholders to ensure that privacy and transparency rights are fully respected throughout the design, operation, and evolution of a digital identity ecosystem in Canada. Ontario Health's privacy and legal team members are working with Ontario Health's business partners, the Ministry and MPBSDP to ensure the program aligns with this resolution and will be consulting with the IPC in support of this.

Increasing Provider Access to Patient Health Records: Provincial Clinical Viewer (PCV) and EHR Clinical Data Foundations (updated)

Ontario Health currently funds and supports three clinical viewers in Ontario that provide overlapping functionality to clinicians but 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 clinical viewer for providers to access health information available in the EHR. This program consists not only of the establishment of the single viewer, PCV, 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 'Individual access to the EHR' above, to account for the individual access requirements, the scope of the Viewer Consolidation Strategy was expanded to also include a provincial patient viewer (**PPV**) to provide individuals with a digital means of access to their EHR information.

The privacy and information security teams have completed preliminary business requirement work for the PCV.

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 Clinical Data Repository (**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.

The Privacy Office is providing privacy requirements, assurance, advisory, risk assessment and impact work to enable all aspect of this complex replacement, development and migration initiative.

The Information Security Office has been engaged and supporting the initiative through planning to execution. Security architectures reviews, Threat and Risk Assessments and pen-tests have been advised and will be conducted to identify potential threats, risks and propose mitigations.

Collaboration to Implement Enhanced and Expanded Cancer Screening Programs (new)

In October 2024, Ontario Health launched an expansion of the Ontario Breast Screening Program that lowered the starting age to 40 from 50. Expansion work required collaboration between Ontario Health's Privacy Office, the Primary and Community-Based Care Portfolio, and Digital Excellence in Health. A privacy impact assessment was completed to enable changes in data collection systems, update analytics reporting products, and launch enhancements to the Ontario Wait Time Reporting Website, allowing people in Ontario who are eligible for screening to locate screening sites that best meet their needs (such as language or accessibility requirements) and providing information on wait times at screening sites.

In March 2025, Ontario Health launched HPV testing as the new enhanced test for the Ontario Cervical Screening Program, replacing the Pap test as the primary screening test for cervical cancer in Ontario. HPV testing is more sensitive and requires testing less often. This transition required privacy support to onboard lab partners, launch new data collection systems and data pathways, and enable new business logic for correspondence campaigns. Privacy impact assessments were completed to support this multi-faceted initiative, as well as regulatory amendments with the Ministry of Health. Complex privacy support was also required to support new agreements, decommission legacy agreements, and to navigate OH's legislative authorities to enable analytics reporting about the new testing.

Artificial Intelligence and Privacy (new)

In the month of April, the OH Learning and Development team, in collaboration with the Cyber Security, Information Security, Privacy, Legal, and Enterprise Products teams, hosted the session *Demystifying AI: Introduction to AI and Its Use at Ontario Health* in April.

An overview was provided of Artificial Intelligence (**AI**), while introducing Ontario Health's Generative Artificial Intelligence Guideline. The session aimed to highlight key topics such as the emerging regulatory landscape, legal risks and legal frameworks, while emphasizing responsible use of AI and the overlapping privacy principles for responsible, trustworthy and privacy protective generative AI technologies.

Privacy actively participates in Ontario Health's Internal AI Committee with a mandate to implement the Responsible Use of Artificial Intelligence Directive. This Provincial Directive applies to all Ontario Ministries and Agencies; applies to all systems that use AI (undefined) as part of the development, delivery of, or decision-making for, a policy, program, or service; and requires disclosure of AI use and the establishment of a risk management framework.

Mental Health and Addictions Provincial Data Set Expansion (new)

The Mental Health and Addictions Centre of Excellence (**MHA CoE**) at Ontario Health supports the development of a comprehensive and connected mental health and addictions system across the province. Over the past year, the Privacy team has supported the MHA COE with the expansion of data collection to deliver on the three pillars with 71 new health serve providers contributing to the Provincial Data Set (**PDS**).

The Privacy team has conducted privacy impact assessments related to new clinical program-specific data sets for priority programs, including depression and anxiety-related conditions, schizophrenia, and psychosis, eating disorders, and substance use disorders. In coordination with the project team, security team has established standards for security assessment before on-boarding new sites for MHA data submission.

The eClaims Expansion (new)

A multitenant release was successfully deployed in the eClaims application and is now in Production. Privacy and Security were key players, providing the project team with ongoing privacy and security consultation. The necessary privacy and security assessments were performed in a timely manner, ensuring smooth delivery. eClaims release 4.0 builds the foundation to make the eClaims application a platform that will support multiple Programs (referred in the application as tenants), which is the scope of the eClaims Expansion project.

Leveraging this platform for other Ontario Health Programs (tenants), where adjudication and reimbursement are fundamental, will enable new programs to be onboarded in this architecturally updated platform. In summary, this release includes updates such as new User Interface screens, enhanced access control, updates to various tables and functions, and updated session timeout.

Health 811 (updated)

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. 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 to ensure Health811 has privacy and security controls in place acceptable to the Ministry, Ontario Health and in accordance with the agreement framework.

Work continues on a value-based incentive framework intending to decrease costs, and demonstrate the value created and outcomes generated by Health811. Both Health811 and Ontario Health privacy, legal and other business team members are working with the Ministry of Health on processes and risk assessments that would permit collection, use and disclosure of existing and new data assets, as well as a robust set of agreements.

Additionally, as part of operating the service and ongoing management, the Ontario Health privacy and security teams informed and supported several pre-business requirements document and business requirements document reviews, including episodic access to care improvements, online appointment booking, unified search and search optimization, and Ontario Breast Screening Program to highlight a few examples.

Leading Projects (updated)

Privacy was a key partner in the planning and work-up conducted with the 7 Leading Projects (**LP**s) that went live in fiscal year 2024/25. Ontario Health as a Health Information Network Provider (**HINP**) was required to make changes and enhancements to CHRIS to allow the system to facilitate the LPs program delivery and was required to conduct seven privacy impact assessments (**PIA**). The PIAs were focused on the Lead Health System Partners (**Lead-HSP**), who were identified to be the CHRIS tenant of the individual Leading Project. The PIAs focused on the Lead-HSP and their interaction with CHRIS for the purposes of the Leading Projects. Ontario Health worked closely with the participating Ontario Health Teams (**OHT**s) (and their Lead-HSP), OHaH and various teams within Ontario Health to conduct these 7 comprehensive PIAs. Findings of the PIAs were integral to establishing policies, processes, and agreements to support implementation of the Leading Projects, including onboarding the Lead-HSP onto the CHRIS system. Ontario Health shared findings of these PIAs with the participating LPs and OHaH. Ontario Health has mitigated all of its privacy risks. The participating LPs are still working to close out some of the risk mitigation strategies that were identified in the PIAs. Leading Projects went live in 2024/25 without CHRIS with plans to onboard onto CHRIS in early Q2 2025/26. The Privacy team will continue to work with supporting partners and programs to support CHRIS onboarding in accordance with PIA findings and recommendation.

Security team has completed the risk assessment for the leading projects as well 20 partners sites to ensure the sites has sufficient implementation of security controls before on-boarding.

CHRIS Services & The Future of Home Care (updated)

The Privacy Office worked closely with the CHRIS product business team to prepare for future home care delivery models through development of a regional hub, moving away for the current model of establishing CHRIS tenants. A PIA was conducted that considered the impact of OHTs use of CHRIS, where they are comprised of more than one health information custodian. Risk findings and recommendations from the PIA were used to inform the Leading Projects work and development of a new HINP agreement framework for CHRIS and related systems and guidelines, and privacy guidelines for CHRIS tenants. The deployment of a regional model of CHRIS in accordance with the recommendations from the PIA, ensure that CHRIS is able to support the work towards provincial work towards home care modernization.

Medical Equipment Supplies (MES) (updated)

The Ontario Ministry of Health (**MOH**) has identified CHRIS within their Digital Health Playbook as a digital asset. While Ontario Health does not directly provide care to Ontario patients, the organization does provide digital programs and tools that allow health care organizations to coordinate the delivery of patient care across multiple regions of Ontario. Accordingly, in effort to modernize the public sector supply chain, procurement of vendors, OHaH executed a number of contracts with vendors for medical equipment supplies (**MES**) which required integration with CHRIS for service delivery.

Ontario Health conducted 12 PIAs to support this work – a PIA assessing the overall enhancements being made to CHRIS to support this work, and 11 PIAs looking at various vendor integrations to CHRIS. The project integration with vendors resulted in automated transfer of purchase orders related to MES to contracted vendors and notification from vendors to OHaH of the fulfilment of purchase orders. Ontario Health successfully completed these 12 PIAs to meet project timelines and worked with various groups internally and with OHaH and vendors to mitigate risks identified through the process.

ISO Security team participated in the procurement process by specifying security requirements and evaluation of the responses. After selection some of the MES partners provided SOC2 Type II reports and others completed NIST based security self-assessment. ISO security team reviewed the documents and ensured that the required applicable security controls are implemented in their environment.

Organ Allocation and Transplant System (OATS), Integrations (updated)

The Organ Allocation and Transplant System (**OATS**) was launched in 2022 by Ontario Health. OATS replaced the legacy system 'TOTAL', which was used by Trillium Gift of Life to manage organ allocation and transplantation in Ontario.

External OATS users, such as staff at transplant hospitals and Human Leucocyte Antigen (**HLA**) labs manually copy patient data from their systems (i.e. EMRs and LIS) into OATS. To enhance the quality of patient care in the transplant journey, Ontario Health worked with the OATS vendor and HLA labs to integrate OATS with Ontario transplant hospitals' EMR systems, which consist of 7 sites, and HLA Lab systems, which consist of 5 sites. The integration will facilitate a one-way transfer of relevant patient data from the transplant hospitals and HLA labs into existing OATS data fields. The integration is intended to replace the current manual input of data by transplant hospitals and HLA Labs staff into OATS, thus improving the quality and integrity of the solution.

The integration will result in:

- The minimization of clinical risk by eliminating or decreasing duplicate documentation and documentation transcription.
- Improved timeliness in accessing patient data between systems.
- More efficient workflows in the reduction of duplicate data entry and minimization redundancies.
- Improved patient outcomes through the capture of accurate patient information.

To support this change, the Privacy Office led development of a PIA to assess the privacy risks and propose recommendations for risk mitigation. The PIA and related work were integral to launching the first integration as a test. The Privacy Office worked closely with legal to develop an agreement framework and has provide privacy expertise to participating programs as they plan to integrate with OATS. Information Security Office conducted a Threat and risk assessment, developed a risk treatment plan and assisted with mitigation of identified risks.

In 2025/26, TGLN will embark on expanding integration for a safer system and processes to support transplantation in accordance with the privacy practices that were called to action through the PIA.

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 has developed certification and compliance processes for approved interoperability specifications to ensure that vendors, health information custodians, and Digital Health Asset owners progress to a standards-based provincially guided interoperability. Privacy and Security assessments were completed on a tool procured to support and automate the certification and compliance processes were completed to identify risks and propose mitigations. In 2024/25, Ontario Health held consultations with the IPC regarding the Digital Health Drug Repository (**DHDR**), Ontario Laboratories Information Systems (**OLIS**), and Surgical Efficiency Reporting Information System (SERIS) interoperability specifications. Ontario Health also received approval for an amendment to the previously approved Acute and Community Clinical Data Repository (**acCDR**) interoperability specification from the Ministry of Health.

Digital Correspondence (updated)

Ontario Health launched an initiative in 2023 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 and Information Security Office were engaged to provide support throughout the entire project lifecycle to ensure Privacy by Design and Security 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 formal privacy risk assessment and threat risk assessment.

Ontarians will be able to choose to receive screening correspondence via a secure online portal, with authentication through the My Ontario Account for Health. For the initial Minimal Viable Product, only colon cancer screening correspondence will be available, and paper correspondence will continue in tandem.

In 2024, end-user feedback was obtained through several engagement sessions, with a short-form Privacy Impact Assessment (**PIA**) conducted to ensure best practices. Throughout 2024 and into 2025, the end-user facing content for the future online portal was created, including privacy content such as Notice of Collection and Terms of Use. A conceptual Privacy Impact Assessment was completed in mid-2024 to analyze the project design decisions to-date, with a comprehensive Privacy Impact Assessment planned for mid-2025. In May 2025, an external vendor was onboarded to complete the build of the online portal and associated APIs, with the Privacy Office being heavily involved in the RFP, vendor selection and SOW processes. A tentative go-live for the online portal is scheduled for Q2 of 2026/27.

Patients before Paperwork – Modernizing Provider Communication (updated)

Ontario Health is working in partnership with the Ministry of Health to develop and implement a comprehensive five-year strategic plan for Patients before Paperwork (**PB4P**). This plan aims to alleviate the administrative burden on physicians in Ontario while enhancing access to healthcare services for Ontarians. As part of this initiative, Ontario Health has identified five primary use cases, namely Referrals and Central Intake, Prescriptions, Lab Requisitions & Results, Medical Notes, and Administrative Processes, which will serve as the foundation for reducing administrative tasks and improving the overall efficiency of healthcare delivery in the province.

As part of the Pb4P initiative, Ontario Health aims to develop an integrated clinical process that incorporates digital communication tools for various healthcare tasks. This includes, exchanging referrals, conducting consultations, ordering lab results and diagnostic imaging tests, and managing central intake processes. The goal is to fully implement this integrated approach and seamless digital solutions within the next five years.

The Privacy team has played an active role in capacity building within the PB4P large-scale provincial initiatives, notably through its substantial involvement in forming a Patient and Family Advisory (**PFA**) committee. This committee is essential for incorporating the patient perspective into the 13 work streams of the PB4P initiative, ensuring that these efforts remain patient-centered and impactful.

To advance the future state eReferral network, Ontario Health successfully established Vendors of Record (**VOR**) through an open and competitive procurement process initiated in November 2023. The Privacy and Security team is presently engaged in supporting the intricate integrations of these VORs with the Provincial Care Coordination Gateway (**PCCG**) and the Provincial Health Services Directory (**PHSD**) in preparation for the upcoming technical go live. These integrations necessitate complex assessments, and the team has conducted five such assessment to support this work. Additionally, the teams assessed the eForms Designer tool as part of the Central Intake work stream to facilitate the digitization of 17 referral forms, enabling the use of digital forms and the new referral network for the go live of Q1 25/26. Furthermore, the team has finalized procurement evaluations for central intake vendors to further improve the future state of eReferral.

The eForms workstream focuses on reducing the administrative burden in Primary, specifically the time spent on filling various forms. The Ontario Medical Association and Ministry of Health Forms working group identified 12 priority forms to implement, starting with the digitized Long-Term Care (**LTC**) Health Assessment Form (**HAF**) to replace the current fax or email submission from Primary Care to OHaH. In February 2024, the eForms limited production release (**LPR**) workstream was launched as part of the PB4P initiative. In support of this initiative, the Privacy team conducted two privacy assessments to facilitate the integration of the eForms solution directly with Electronic Medical Records (**EMRs**). Additionally, the privacy and security team assisted in assessing the capability to enable Health Information Custodians lacking digital means to submit forms through the eForms solution using the web-based service, One Health Launcher. This support aims to ensure a seamless transition to digital form submissions and enhance overall efficiency in the Primary Care setting. Throughout the fiscal year, the privacy and information security teams were actively involved in supporting the launches of Referrals and Central Intake and Administrative Processes. Work on these initiatives continues, as the Privacy Office and Information Security Office remains actively engaged in ongoing efforts to support the transformation of how Ontarians receive access to healthcare.

Privacy and Security by the Numbers: Key Metrics

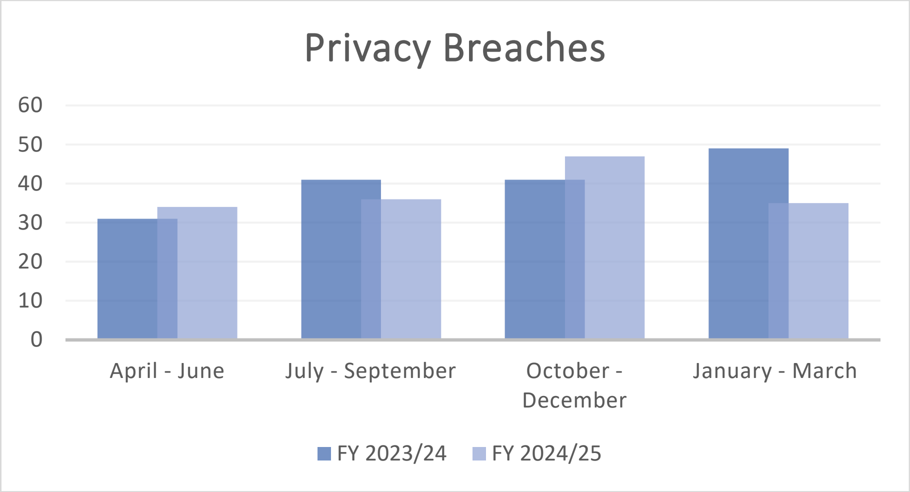
The following key privacy and security metrics highlight some of the work accomplished by the privacy and information security teams in 2024/2025 and provides a measure of Ontario Health's compliance with legislative and regulatory requirements as well as with respective information practices.

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 27.3 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 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.



Overall, Ontario Health saw a slight decrease in the number of breaches reported during 2024/25[3].

[3] Please note that Contact Centre Screening Program incidents are not included in the chart; and are reported separately in the section "Ontario Cancer Screening Program – Misdirected Correspondence".

Ontario Cancer Screening Program – Misdirected Correspondence

Over the 2024/25 fiscal year, Ontario Health mailed approximately 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. There was a slight increase in the amount of correspondence which were delivered to an outdated or incorrect address and returned to Ontario Health, being 519 in 2023/2024, compared to 738 in 2024/2025. Misdirected, misdelivered or opened correspondence represents only 0.01% 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 also sends 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.

EHR Access & Correction Requests and Consent Directive Requests

Processing 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.

Access and Correction Requests				
	April - June	July -September	October – December	January - March
FY 2023/24	129	121	108	154
FY 2024/25	139	114	111	137

Consent Directive Requests				
	April - June	July -September	October – December	January - March
FY 2023/24	143	101	138	109
FY 2024/25	129	192	110	566

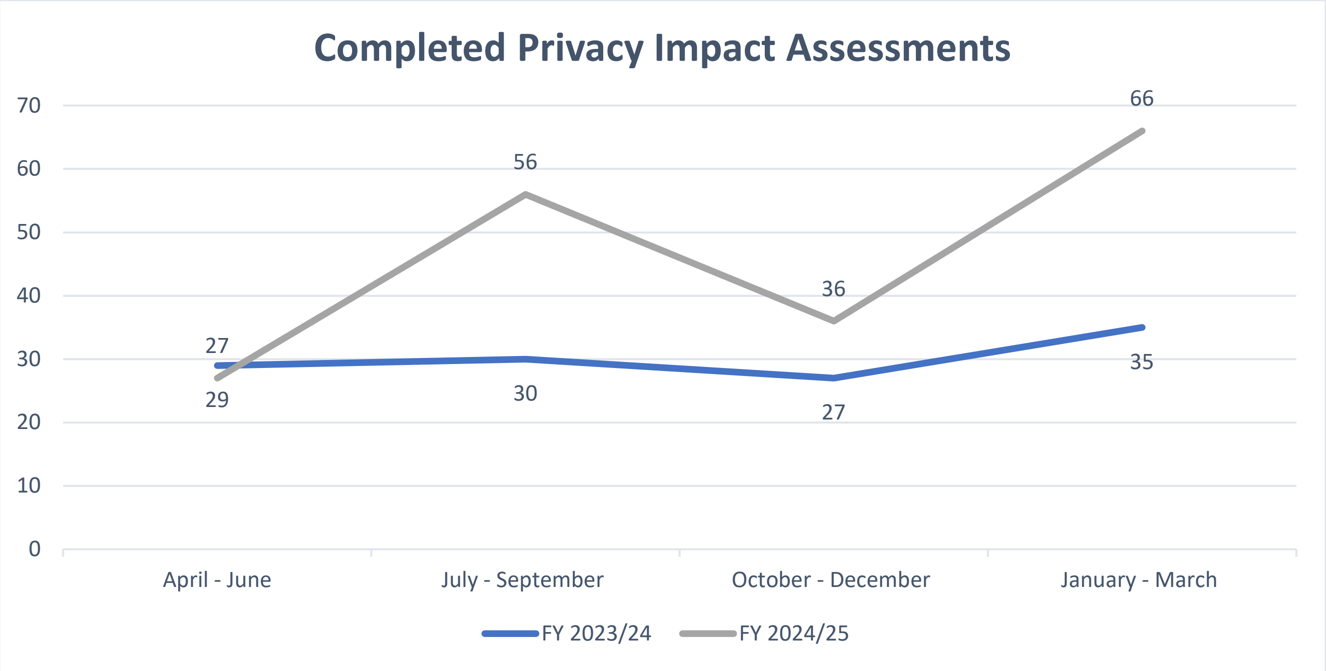
EHR Privacy Incident Management – Health Information Custodians and Coroners

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 (**HIC**) 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 Reported Privacy Breaches				
	April - June	July -September	October – December	January - March
FY 2023/24	19	12	11	14
FY 2024/25	17	11	18	9

Privacy Impact Assessments

Last fiscal year, Ontario Health conducted or provided oversight for the conduct of 185 PIAs compared to 121 the year prior. A key obligation and function performed by the Privacy Office is the completion of PIAs that serve to assess new or updates to legislation or regulation, programs, services, processes, 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.



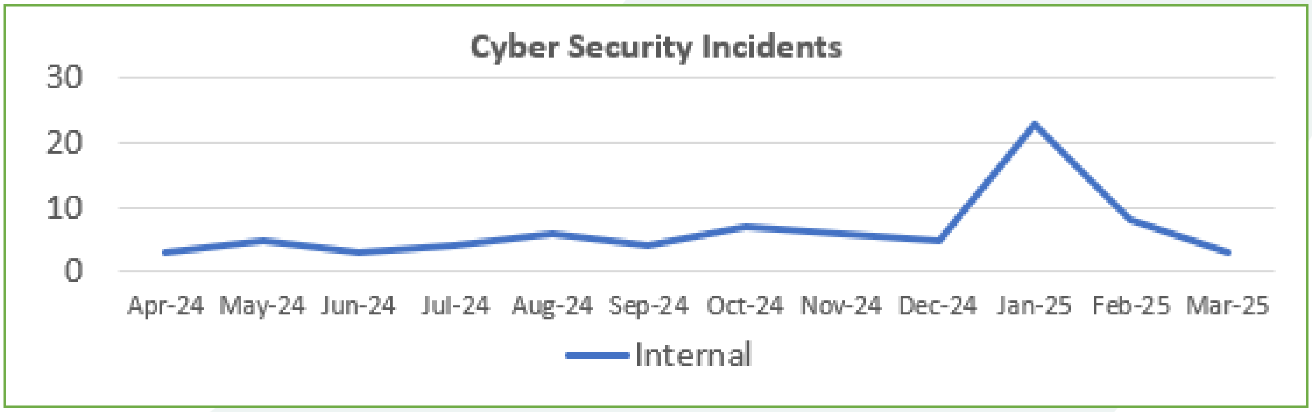
The significant increase in PIAs since the previous fiscal year is attributed in part to the large volume of high priority initiatives related to (i) OHT deployment (Leading Projects - 7 PIAs) and (ii) modernization of the public sector supply chain via system integrations (Medical Equipment and Supplies - 11 PIAs). These PIAs in particular, will be foundational and support any subsequent OHT deployment onto CHRIS and CHRIS vendor system integrations related to Medical Equipment and Supplies.

Security by the Numbers: Key Metrics

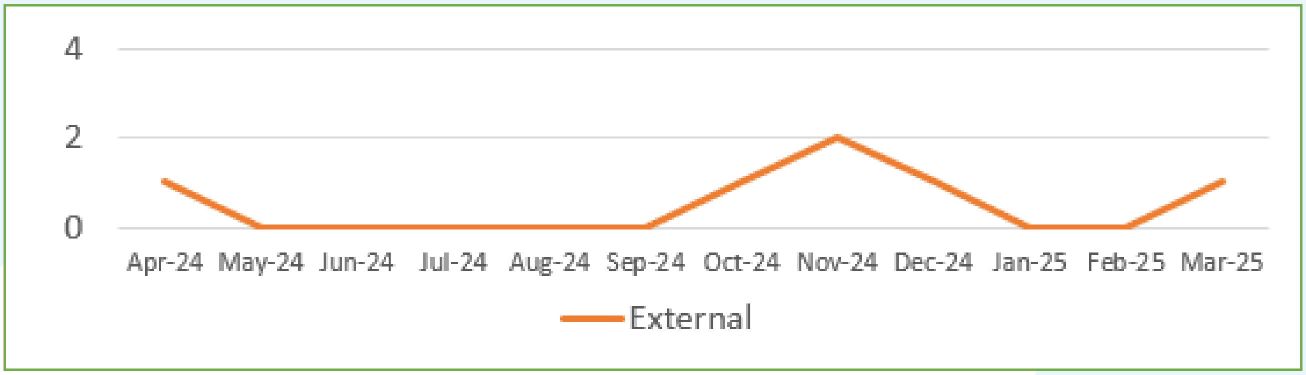
Cyber Security Incidents

During the period of April 2024 to March 2025, internal incidents, characterized predominantly by low severity, have stemmed largely from non-authorized user activities such as attempts to connect to malicious URLs or failed authentication attempts from unfamiliar locations. These incidents are effectively detected and blocked early by automated cyber tools, ensuring minimal impact on Ontario Health’s assets. Despite the low severity, all internal incidents are tracked meticulously across all severity levels, confirming the robustness of Ontario Health’s internal monitoring mechanisms.

On the external front, the trend of reported incidents has seen an overall decrease. The majority of these incidents, which were reported from the sector and classified with higher severity, have not affected Ontario Health assets. This decline is indicative of the success of the education and guidance provided by Ontario Health, which has significantly bolstered cyber security awareness among external entities, leading to improved response to containment and eradication measures. The notable spike in Q4 it did not impact the broader downward trend of incidents.



Internal Cyber Security Incidents: Internal cyber security incidents are classified as true-positive attacks, involving malicious activities aimed at compromising Ontario Health's systems. Most of these incidents range from low to medium severity, thanks to the efficacy of automated cyber security defenses in detecting and blocking such activities promptly.



External Cyber Security Incidents: External incidents are typically of high severity and are reported to Ontario Health when malicious attacks necessitate system shutdowns. Although these incidents pose a risk to Ontario Health's systems, this risk is mitigated through robust cyber security defenses and active collaboration with the affected external organizations.

Threat Risk Assessments

The security metrics below provide information on number of completed internal and external Threat Risk Assessments (**TRAs**), security assessments and penetration tests conducted on new systems or operational changes. Additionally, to comply with industry best practices and standards, the figures below detail the number of full vulnerability scans performed across various network infrastructures within Ontario Health.

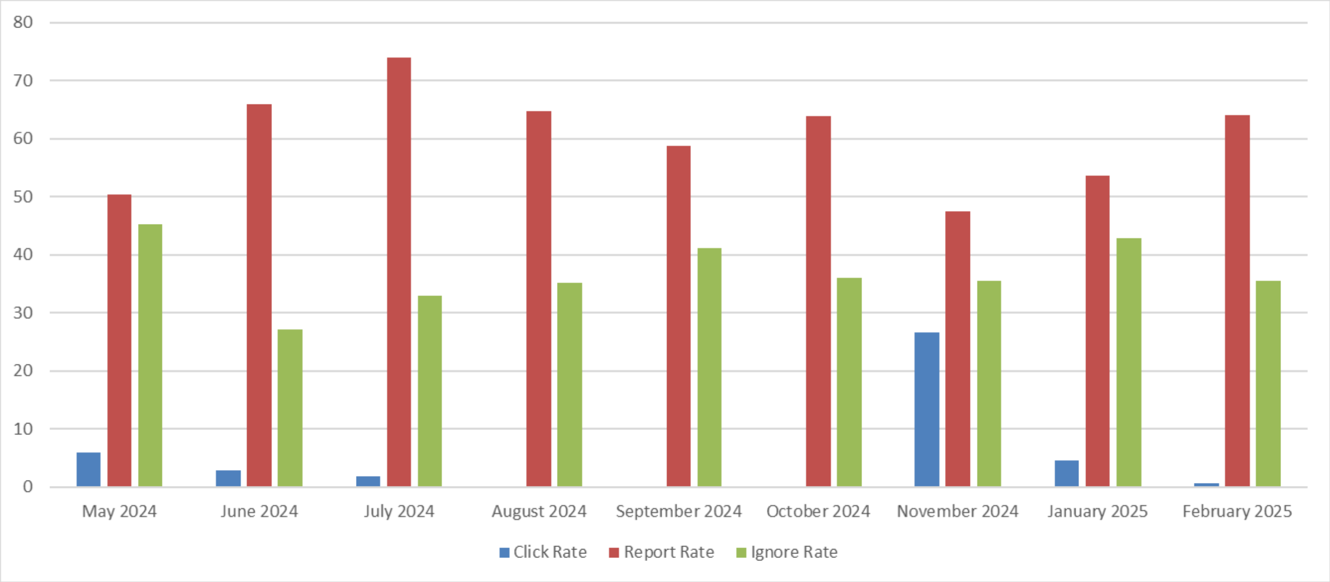
During fiscal year 2024-2025, the ISO completed (executed & reviewed) more than 150 security assessments for more than 50 projects.

Key Cyber Security Activities - 2024-2025 (RISK MANAGEMENT)				
	Internal TRA	**External TRA**	**Security Assessments**	**Penetration Test**
Completed Number of Assessments by Type	5	10	20	8

Key Cyber Security Activities - 2024-2025 (RISK MANAGEMENT)				
EHR Specific Assessments	**NIST (Self Assessments)**	**TRA** Review	**Penetration Test** Review	**Vulnerability Scan (VA Scan)** Review
Completed Number of Assessments by Type	50	20	15	30

Ontario Health Phishing Simulations Campaign Results

During fiscal year 2024-2025, Ontario Health's phishing awareness campaigns continue to show measurable improvement in user vigilance and response. The campaigns tracked four key performance metrics: click rate, report rate, ignore rate and remediation rate—to assess engagement and inform future awareness strategies. Click rates steadily declined from 5.9% in May to near-zero levels by February, showing reduced susceptibility to phishing attempts. While a notable spike to 26.7% occurred in November—attributed to a purposefully challenging phishing simulation which served as a valuable stress test for user awareness. At the same time, report rates remained strong, with highs of 74% in July and 64.5% in February, indicating increased user confidence in identifying and reporting suspicious emails.



The ignore rate fluctuated between 27% and 43%, suggesting an opportunity to further engage a cautious but passive segment of users through targeted awareness efforts. Encouragingly, post-click remediation rates remained consistently high, with 100% training completion in multiple months, reinforcing Ontario Health's ability to respond effectively and close awareness gaps. Overall, these trends reflect a maturing security culture—one that prioritizes awareness, timely reporting and continuous improvement in safeguarding against email-based threats.

Phishing campaign results are tied to monthly phishing campaigns where simulated malicious emails are sent to employees. A high report rate and low click rate is the desired outcome. While ignore rate does not pose a direct security risk, it is also not the optimal action. A high report rate indicates that staff are security aware. A low click rate is attributed to effective awareness and training initiatives. As complexity increases, these results can be impacted. The campaigns are applied uniformly across Ontario Health with varying complexity.

Looking Forward

To continue delivering on its core mandate of integrating the health system and supporting superior patient-centered care, Ontario Health requires data – PHI and PI. 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 additional key 2025/2026 priorities (in addition to the on-going work described above) for the privacy and cyber security teams.

TGLN Information Systems (updated)

Considerable work was undertaken to support finalization of the Donor Management System (**DMS**) vendor contract in late 2024/25. With the new contract in place, the Privacy Office is positioned to undertake a comprehensive PIA of the end-to-end donor management system. Additionally, as OATS integrations progress, work is already underway to support the next phases of OATS development. The Privacy Office will be integral to ensuring privacy compliance and privacy by design principles are incorporated into the subsequent development of the OATS system. This will entail updating existing PIAs.

Health Care Connect (new)

The Health Care Connect (**HCC**) program was established in 2009 by the Ministry of Health to connect unattached patients to primary care practitioners and increase the overall attachment rate in Ontario. The program allows people without a regular family health care provider, to register for assistance in finding physicians and nurse practitioners who are accepting new patients in their community.
In support of the Primary Care Action Team (**PCAT**) mandate and in preparation for future enhancements to the HCC program, The Ministry requested OH privacy resources to conduct a review of existing privacy controls currently in place for the end-to-end HCC program, identity potential gaps and recommend activities to address any gaps. The Ministry also requested OH privacy conduct a privacy impact assessment which is currently in progress.

Enhancing Cyber and Operational Resilience: Integrating Shared Capabilities, Defense Strategies and Training for a Secure Culture (new)

In fiscal year 2025-2026, the Ontario Health Cyber Security Program will prioritize a number of key initiatives when it comes to cyber security defense and information security aimed at enhanced security and operational resilience within the organization:

- **The Zero Touch Certificates and Key Management Program (ZTKMP)'s Focus on Automation and Cryptography:** Deepening automation, enhancing cryptographic agility and expanding readiness for post-quantum technology. Key initiatives include, extending TLS certificate rotation and automating key lifecycle management.

- **CIMP's Proactive Measures:** Expand its scope to include threat hunting and advanced analytics. The program will refine incident response plans and enhance collaboration with external partners to address evolving cyber threats.

- **EIAM's Integration and Security Enhancements:** Integrate identity management framework, expanding multi-factor authentication and single sign-on coverage, and conducting audits to identify vulnerabilities.

- **Netskope Solution:** Expand integration with other security tools like Microsoft Defender and Saviynt to further enhance the organization’s security posture.

- **Microsoft Preview:** Broaden the deployment of Microsoft Purview to cover additional areas such as cloud file shares, Teams, SharePoint, PDF files and Power BI. The focus will be on tagging data assets for classification and developing data loss prevention policies to support data governance.
- **Elevating Security Posture:** Refining Ontario Health's adaptive strategies to emerging threats and working towards ensuring that our systems are resilient against cyber attacks. Key areas of focus will include expanding our product-focused vulnerability management, enhancing our SOC capabilities and further optimizing our identity protection frameworks. Through these efforts, we aim to stay ahead of the curve in cyber security, safeguarding our organization's digital assets and supporting its long-term objectives.
- **Expanding Application Security Testing:** Expand DAST implementations across various facets of our operations. Security testing will begin in the Ontario Health on-premise environments, targeting both new and existing applications to ensure thorough vulnerability assessments and remediation protocols. Additionally, we plan to refine and optimize DAST processes within our cloud Azure subscriptions. This involves enhancing integration mechanisms, increasing the frequency of security scans, and leveraging advanced analytical tools to derive actionable insights from the scan results.
- **Cyber Threat Simulation and Resilience:** Currently, Ontario Health conducts ad-hoc Tabletop Exercises (**TTX**) and Penetration Testing (**Pentest**). However, in fiscal year 2025-2026, we plan to procure tools that will enable Ontario Health to perform these exercises more frequently, with greater scope flexibility and regular scheduling, thereby improving preparedness and resilience.
  - The TTX function will allow leadership and key stakeholders to simulate and navigate high-impact cyber incidents in a structured, discussion-based format. These exercises will help shape strategic decision-making, clarify roles and responsibilities, and enhance the organization's readiness for unforeseen events.
  - The Pentest capability (Red/Purple teaming) will provide targeted assessments of information systems, identify potentially exploitable vulnerabilities, assist in prioritizing the remediation of these vulnerabilities, and assess/improve the effectiveness of existing security controls.
- **Advancing Phishing Campaigns:** Introduce new strategies to strengthen defenses against phishing attacks. Plans include an updated employee training module on emerging tactics, collaboration with external cyber security experts and continuous monitoring with adaptive security protocols. Our goal is to foster a security-conscious culture and maintain vigilance at all levels.

Boosting cyber resilience through shared capabilities and controls remains critical for Ontario Health and its work to further operationalize the Provincial Cyber Security Operating Model throughout the health care sector. Looking ahead, Ontario Health will focus its efforts aimed at enhancing resilience for the health care sector through the following initiatives:

Progress the Provincial Cyber Security Operating Model Beyond Acute Hospitals

- Continued development of the model's strategy into primary care, long-term care and public health

Enhance Critical Controls Tracker

- Support health service providers develop and execute roadmaps for target state maturity of critical control implementation.

Continued Optimization of CSOM Provincial Platforms

- Increase partner and service provider participation in the Cyber Threat Intelligence Exchange (**CTIX**) platform.
- Operationalize updates from the provincial cyber security maturity platform, including enhanced user functionality, interface, and reporting capabilities.

Operationalize Proactive Hardening and Attack Surface Reduction (PHASR)

- Determine opportunities for collaboration and partnership with the Ministry of Public and Business Service Delivery and Procurement's Cyber Security Centre of Excellence on the future of the health sector's adoption of the provincial attack reduction service solution.

Ontario Health is committed to expanding its security infrastructure by implementing advanced threat intelligence systems and extending protection to emerging digital platforms. The organization is investing in enhanced monitoring tools to enable real-time detection and response to cyber threats, ensuring proactive defense mechanisms. Additionally, Ontario Health will continue to strengthen partnerships with cyber security organizations and experts to stay ahead of evolving threats and leverage cutting-edge technologies. Continuous improvement programs will be initiated to refine security protocols and strategies based on the latest industry trends and threat landscapes.

Acroynms

Acronym	Meaning
3LOD	Three Lines of Defense
acCDR	Acute and Community Clinical Data Repository
AI	Artificial Intelligence
CDF	Clinical Data Foundations
CDR	Clinical Data Repository
CHRIS	Client Health-Related Information System
CPAM	Cloud Privileged Access Management
CPO	Chief Privacy Officer
CSD	Cyber Security Defense
CSF	Cyber Security Framework
CSIR-MP	Cyber Security Incident Response Management Program
CSOM	Cyber Security Operating Model
CTIX	Cyber Threat Intelligence Exchange
DAST	Dynamic Application Security Scanner
DCIS	Data Collection Information System
DI-CS	Diagnostic Imaging-Common Service
DHDR	Digital Health Drug Repository
DHI	Digital Health Identity
DHIEX	Digital Health Information Exchange
DMS	Donor Management System
EDR	Endpoint Detection & Response
EDSTA	Enhancing Digital Security and Trust Act
EHR	Electronic Health Record
EIAM	Enterprise Identity and Access Management
EMR	Electronic Medical Record
ESP	Electronic Service Provider
FIPPA	*Freedom of Information and Protection of Privacy Act*
FOI	Freedom of Information
GRC	Governance, Risk, and Compliance
H811	Health 811
HAF	Health Assessment Form
HCC	Health Care Connect
HIC	Health Information Custodian
HINP	Health Information Network Provider
HLA	Human Leucocyte Antigen
HSP	Health Service Providers
HSPS	Health System and Performance and Support
IAM	Identity and Access Management
IGA	Identity Governance and Administration
IPC	Office of the Information and Privacy Commissioner of Ontario

ISO	Information Security Office
ISSC	Information Security Steering Committee
ISKE	Information Security Knowledge Exchange
Lead-HSP	Lead Health System Partner
LP	Leading Projects
LPR	Limited Production Release
LTC	Long-Term Care
MFA	Multi Factor Authentication
MSSP	Managed Security Service Provider
MES	Medical Equipment Supplies
MOH	Ministry of Health
MPBSDP	Ministry of Public and Business Service Delivery and Procurement
NIST	National Institute of Standards and Technology
O. Reg.	Ontario Regulation
OATS	Organ Allocation Transplant System
OCSR	Ontario Cancer Screening Registry
OHDC	Ontario Health Data Council
OHCSC	Ontario Health Cyber Security Centre
OHT	Ontario Health Team
OLIS	Ontario Laboratories Information System
ORN	Ontario Renal Network
OS	Operating System
PB4P	Patients Before Paperwork
PCAT	Primary Care Action Team
PCCG	Provincial Care Coordination Gateway
PCV	Provincial Clinical Viewer
PE	Prescribed Entity
PFA	Patient and Family Advisory
PHDDS	Provincial Health Data and Digital Service
PHI	Personal Health Information
PHIPA	*Personal Health Information Protection Act*
PHSD	Provincial Health Services Directory
PI	Personal Information
PIA	Privacy Impact Assessment
PO	Prescribed Organization
POV	Proof of Value
PP	Prescribed Person
PPV	Provincial Patient Viewer
RBAC	Role Based Access Control
RROSH	Real risk of significant harm
SaaS	Software-as-a-Service
SERIS	Surgical Efficiency Reporting Information System
SOC	Security Operations Centre
SSO	Single Sign - On

TGLN	Trillium Gift of Life Network
TRA	Threat Risk Assessment
TTX	Table-Top Exercise
VOR	Vendor of Record
ZTKMP	Zero Touch Certificates and Key Management Program

Need this information in an accessible format? 1-877-280-8538, TTY 1-800-855-0511, info@ontariohealth.ca.
Document disponible en français en contactant info@ontariohealth.ca