2020/21 Ontario Health Annual Privacy and Security Report
Contents
1. Introduction .......................................................................................................................... 3
2. Background .......................................................................................................................... 4
3. Key Privacy and Security Milestones and Achievements ....................................................... 8
4. Key Program Initiatives ......................................................................................................... 11
5. Privacy and Security by the Numbers: Key Metrics .............................................................. 14
6. Looking Forward ................................................................................................................... 16
1. 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 and Protection Act (PHIPA) and the Freedom of Information and Protection of Privacy Act (FIPPA), and is committed to respecting the privacy rights of individuals, safeguarding their information and complying with Ontario’s privacy laws.

As a newly formed agency, Ontario Health continues to undergo a period of transformation and structural change. Since its formation in 2019, the privacy and information security teams have worked diligently to integrate the privacy and security programs of several provincial agencies. Through these transfers Ontario Health has assumed multiple PHIPA roles and a complex regulatory framework which it must navigate to maintain a trust model and optimize the use of data for good as it transforms the health system.

As Ontario Health matures and evolves as an organization, it also continues to respond to changing demands and new developments in the Ontario healthcare system by supporting the province’s response to COVID-19, adapting to changes in the privacy regulatory landscape and enabling the Ministry of Health’s Digital First Strategy. During this time the Privacy Office and Information Security Office have leveraged its considerable expertise and experience to support Ontario Health’s strategy, by creating harmonized information practices that will optimize the responsible use of data. In doing so, the privacy and security teams rely on a person and patient centered approach to privacy and security that fosters trust in a world of rapidly evolving technology.

2020/21 has been a unique yet productive year for Ontario Health as it’s privacy and information security teams work together to address the data privacy, integrity, interoperability and compliance matters as it integrates the significant and highly regulated data stores from agencies that have transferred. This Annual Privacy and Security Report describes Ontario Health’s privacy and security programs and highlights its legislative framework and milestones achieved in 2020/21 fiscal year that support and advance Ontario Health in achieving its mandate. The report also takes a look back at key metrics and a look forward at privacy and security priorities for 2021/22.
2. Background

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

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

Through collaboration with various internal and external stakeholders, the Cyber Security Program ensures that security is a key component of all system implementation phases, from inception to implementation and operations.
Privacy Program
Ontario Health is committed to respecting personal privacy and safeguarding the PHI and PI that it has in its custody and control. To support this commitment, Ontario Health has a robust privacy program designed to ensure a privacy culture is not only established but also anchored across the agency allowing it to operate in accordance with its legal obligations and responsibilities. Ontario Health believes that legislation is the floor and not the ceiling for driving compliance. As such it maintains as a foundation ‘Privacy by Design’ principles and industry standards, that help build trust and foster innovation. Ontario Health must continuously earn and maintain the trust and confidence of Ontarians as well as its key stakeholders and partners in order to fulfill its mandate.

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

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

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

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

Prescribed Person (PP)
Ontario Health is also designated as a ‘prescribed person’ for the purposes of subsection 39(1)(c) of PHIPA with respect to its role in compiling and maintaining screening information for colorectal, cervical and breast cancer in the Ontario Cancer Screening Registry (OCSR) under subsection 13(1) of O. Reg. 329/04. This designation grants Ontario Health the authority to collect, use and disclose PHI for the purposes of facilitating or improving the provision of health care with respect to the OCSR.

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

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

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

Researcher
Ontario Health operates a research program to develop new knowledge through epidemiological, intervention, health services, surveillance, and policy research, as well as knowledge synthesis and dissemination. Ontario Health can use PHI it collected as a prescribed entity or a prescribed person for the purposes of research, subject to restrictions and conditions set out in PHIPA.
Electronic Service Provider (ESP) and Health Information Network Provider (HINP)
Ontario Health provides electronic information services to health information custodians to enable them to collect, use, modify, disclose, retain, or dispose of PHI, and/or to exchange PHI with each other. In providing such services, Ontario Health is acting as an ESP and/or HINP, pursuant to O. Reg. 329/04, s. 6 (1) and 6(2) of PHIPA. These roles strictly limit Ontario Health’s use of PHI to that which is required to support electronic services to custodians. Ontario Health provides many application services as a HINP, including the Client Health and Related Information System (CHRIS), as well as eConsult technology that enable health care providers and organizations to share PHI for health care purposes.

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

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

Changing Regulatory Landscape
Ontario’s privacy regulatory landscape is changing faster in the last few years in an effort to balance protections while providing supports for the benefits of patients. These changes directly impact Ontario Health and the many important roles it has in supporting patients and health care providers, the Ministry of Health, and researchers so data can be used for the benefit of all in improving patient care. Over the past year, Ontario Health has taken on new roles and responsibilities under PHIPA, including as a prescribed organization in respect to the development and management of the electronic health record (EHR), and in respect to its role and responsibility for specifying the ways in which “digital health assets” must be interoperable with one another. These new roles are described further in the IPC’s guidance document issued May 2021, entitled ‘Digital Health under PHIPA: A Selected Overview” available at https://www.ipc.on.ca/wp-content/uploads/2021/05/digital-health-under-phipa.pdf. As healthcare transformation and PHIPA modernization progress, Ontario Health continues to stay committed to protecting public trust and
interest through privacy, information security and responsible data governance while enabling the full potential of data.

**Ministry of Health’s Digital First Strategy**

Ontario is leading the operationalization of the Digital First for Health strategy to improve care for all Ontarians through:

- More virtual care options;
- Expanded access to online appointment booking;
- Greater data access for patients;
- Better, more connected tools for frontline providers; and
- Data integration and predictive analytics.

The proposed changes will ensure organizations such as Ontario Health, can collect, use, and share information to allow for better patient care and outcomes while clearly outlining how access to information is protected and remains private and secure. The Ministry of Health’s Digital First Strategy will be supported through proposed changes Ontario is making to modernize PHIPA. As PHIPA modernization continues, Ontario Health looks forward to ongoing consultation with the Ministry and the Information and Privacy Commissioner (IPC) to enable a broader use of data within the organization, and across the health sector in Ontario to achieve its objectives as set in the *Connecting Care Act* and *Gift of Life Act*.

### 3. Key Privacy and Security Milestones and Achievements

In 2020/21, the privacy and security teams focused on achieving the following goals.

**Ontario Health’s participation in the Information and Privacy Commissioner (IPC) Strategic Advisory Committee**

The shift towards increased digitization since the onset of the COVID-19 pandemic is having a profound impact on how Ontarians interact with their governments. It is also changing how public institutions deliver services, either alone or with third-party service providers. This rapid uptake of digital services brings significant privacy and access to information issues that affect us all. It is more important than ever to have a solid plan in place to meet these challenges.

In 2020, the Chief Executive Officer (CEO) of Ontario Health was engaged in a strategic planning exercise with the IPC in order to inform its five-year strategic plan and priorities. The committee brought together access and privacy experts from a diverse range of fields to provide feedback on the priorities that will focus the IPC’s work for the next five years. The committee was comprised of independent advisors, informed by their in-depth knowledge and relevant experiences, members of this committee provide valuable non-binding strategic advice. Ontario Health also participated in the IPC’s public consultation process in respect of its strategic priorities.
Prescribed Entity and Prescribed Person Triennial Review and Approval

Ontario Health must have its information management practices that relate to its prescribed entity and prescribed person role reviewed and approved by the IPC every three years. The privacy and security team have been very active during 2020 working in close collaboration with business teams across Ontario Health to secure the new three-year approval granted by the IPC. In October of 2020 Ontario Health received the approval letter from the IPC, which included the following two recommendations to further enhance the agency’s information practices:

1) Ontario Health should amend its information practices to reflect the agency’s new governance and accountability framework with accountability resting with the Ontario Health Chief Executive Officer by October 31, 2021; and

2) Ontario Health should continue to progress its de-identification program focusing on implementing controls to ensure the least amount of PHI is used where the use of de-identified data is not possible. This should be completed by October 31, 2022.

The Privacy Office and Information Security Office, working with the Data Acquisition team, has continued to demonstrate progress towards these recommendations over the last year.

Ontario Health Prescribed Organization Designation under O. Reg. 329/04 and Submission of Information Practices

On October 1, 2020, Ontario Health was proclaimed as a prescribed organization to develop and maintain the EHR in accordance with Part V.1 of the PHIPA. As a prescribed organization, Ontario Health must have in place and comply with practices and procedures to protect the privacy of individuals whose PHI is received for the purpose of developing and maintaining the EHR, and, for maintaining the confidentiality and security of that information. These practices and procedures must be reviewed and approved by the IPC initially within one year of Ontario Health being proclaimed as a prescribed organization and must be reviewed and approved by the IPC every three years thereafter.

The IPC has provided Ontario Health with a second Manual, the Manual for the Review and Approval of Prescribed Organizations that outlines over 150 pages of policy and procedural requirements that must be complied with, relating to the operations of business teams across the agency including privacy, information security, facilities, human resources, business continuity, disaster recovery, enterprise risk management, product management, data management, account management and legal. The Privacy Office and Information Security Office has worked diligently and collaboratively with staff across the agency to have these information practices prepared for the IPC by the required submission timelines. The IPC will review these practices as submitted by Ontario Health in a phased approach, starting from April 1st, 2021 to July 14th, 2021. OH is anticipating approval from the IPC by October 1, 2021 to continue operating as a prescribed organization.
Privacy Program Advisory Committee (PPAC)
In 2020 the PPAC, consisting of staff from the privacy, legal, security, governance, and digital lead teams across the agency, was re-established to address privacy matters, build trust, breed innovation, and remove barriers to meeting Ontario Health’s mandate. The purpose of PPAC includes to:

- Develop an integrated privacy program for Ontario Health;
- Provide advice on privacy legislative and regulatory amendments; and
- Review and provide feedback on Ontario Health enterprise privacy assessments.

As the privacy program continues to evolve and mature, PPAC will remain a key enabler to ensuring Ontario Health meets its commitments to protect the privacy of Ontarians.

Provincial Cyber Security Operating Model
In 2020/21, Ontario Health initiated a body of work to establish both an Ontario Health cyber security operating model, as well as a cyber security target operating model for health care within the Province of Ontario. These two initiatives were significant for the following key reasons:

- With the transformation of the legacy agencies forming Ontario Health, there was an opportunity to consolidate and benefit from the cyber security capabilities built to service the EHR, as well as adopt new ways of embedding cyber security throughout the organization structure.
- By collaborating with a broad range of public sector digital and security professions, as well as key Digital Health resources, Ontario Health was able to establish a target cyber security operating model for health care in Ontario. This significant first step will allow for the alignment of efforts and investment for both new and established cyber security capabilities.
- Both the internal Ontario Health work and the provincial work align and open further opportunities for synergy at a provincial, regional, and local level.

Cyber Security Program Testing
The establishment of a harmonized Ontario Health cyber security program presented several opportunities to establish new policies and practices. During 20/21, the incident response practices were enhanced and tested through both tabletop exercises and lessons learned from the incident response team.

Harmonized Cyber Security Capability & Service Development
The cyber security gap assessment of each business units and aggregation of the results in conjunction with conducting a full threat risk assessment for Ontario Health enabled resulted in development of the first comprehensive cyber security risk register for Ontario Health. This work enabled the Information Security Office to develop a Capability Model based on NIST framework, in which the required cyber security controls and services have been identified and rolled up to different capabilities in order to mitigate the identified risks in the Risk Register, and allowing the Information Security Office to develop a three years roadmap for improving Ontario Health’s overall cyber security posture.
Data Centre Migrations
To improve system resilience, ensure availability, and increase value, Ontario Health undertook work to both consolidate existing physical data centres as well as continue to embrace Cloud technologies. This two-pronged strategy ensures that where systems are best suited to operate within a data centre, Ontario Health can leverage a pair of robust primary/secondary data centres within Ontario; while also offering a path to migrate systems to security Cloud tenants to obtain greater resilience and value.

4. Key Program Initiatives
The Privacy Office in collaboration with the cyber security and other business partners is responsible to protect individual privacy and the confidentiality, security and availability of data assets and to enable the agency to use data and other assets in support of its programs including the following COVID-19 and other priority initiatives in 2020-2021.

A sample of these programs and initiatives are listed below.

Virtual Visits Vendor Verification Program
The Virtual Visit Verification Program has been established by Ontario Health to give clinicians and healthcare organizations in Ontario access to expanded options for virtual care in support of the province’s Digital First for Health strategy and to support health services planning.

Ontario Health moved forward with Phase 1 in November 2020 which looked at an attestation model. This model requires vendors to self-attest to meeting mandatory solutions requirements (privacy, security & technical). Future phases being conducted in 2021 will require Ontario Health to validate and test those requirements to provide a level of assurance that the vendors are meeting those requirements. This program is being established with close consultation with the IPC.

In 2021 the IPC introduced a new guide on ‘Privacy and Security Considerations for Virtual Health Care Visits’. This Guide provides advice for health care professionals operating in a virtual care context. The IPC sought feedback from the Population Health and Value-Based Systems portfolio on the content of the Guide.

Digital Health Information Exchange (DHIEX)
Enabling the sharing of electronic information between health information custodians is critical to providing Ontarians with efficient, integrated health care. PHIPA was recently amended in January 1, 2021 to facilitate interoperability between the electronic systems. Under these amendments, Ontario Health is responsible for defining interoperability requirements (including privacy and security) for electronic systems, determining specifications, and actively working with vendors and health information custodians through a program to monitor and ensure compliance. As practices mature over time, an increasing number of systems will be subject to mandatory compliance with the interoperability standards established by Ontario Health. Vendor certification will become an
essential service to verify vendors are supporting health information custodians' interoperability requirements.

**Bundled Care Sites – Access to CHRIS**

Bundled Care is a service delivery and funding model in which a single payment is made to cover all care needs of a specific patient for a specific health issue. This means that an organization or hospital approved for Bundled Care may provide not only its customary health care services but also related home care services. Bundled Care home care services are to be managed within the Client Health and Related Information System (CHRIS), which is the home and community care electronic platform provided by Ontario Health. To support Bundled Care sites, the privacy team developed a new agreement framework to facilitate new participants to the CHRIS platform, and conducted related privacy assessments.

**Provider Gateway (ONE Access Gateway – Provider Gateway)**

In 2020/21, Ontario Health implemented a provincial gateway in order to provide an application programming interface (API)-based entry point for health care provider applications and software to access provincial health assets, including electronic health record (EHR) systems and information. It is expected that a large number of applications will start to use the solution over the coming years, and it enables health care providers to have trusted and secure API-based access to electronic health information and services, including but not limited to EHR information. To support the implementation of the Provider Gateway, the privacy team conducted a thorough privacy assessment including a review of the Provider Gateway’s audit and logging behaviour.

**COVID-19 Response**

In response to the pandemic, Ontario Health was tasked with supporting the Ministry of Health in bringing together partner organizations across the health sector to provide evidence-based guidance, coordinate health system process improvements, and facilitate health system services in a rapidly evolving environment. Ontario Health’s work supporting the province’s pandemic response, which is ongoing, has included the delivery several initiatives, some of which are described further below:

- COVID-19 Patient Viewer
- COVID-19 Case and Contact Management
- Funding COVID mobile testing and lab services
- Digital Health Drug Repository (DHDR) – COVaxON data feed
- OLIS Lab Automation
- Mobile Order and Results Entry (MORE)
- Ontario Health Data Platform (OHDP)
- Ontario Virtual Care Clinic (OVCC)
- Internet Cognitive Behavioral Therapy (iCBT)
These initiatives require close review from the Privacy Office and Information Security Office to ensure controls are built into the design of digital services and data analysis, by developing privacy and security requirements, conducting privacy and security assessments, evaluating the privacy and security posture of third-party service providers, and establishing data sharing agreements to govern the collection, use and disclosure of PHI and PI.

**Ontario Data Health Platform (ODHP)**

OHDP is a federated high-performance computing environment for secure, accurate, and privacy-protective linkage of large health data sets that are currently held across various organizations to allow for big data analytics, including machine learning, that will strengthen evidence for Ontario’s ongoing response to COVID-19 and its related impacts.

The July 30, 2020 amendments to s. 18 of O. Reg. 329/04 under PHIPA require Ontario Health as a prescribed entity to disclose PHI to the Ministry of Health when requested by the Minister. This amendment is in force for two years. Ontario Health has had multiple roles within the initiative including participation in the Joint Ministers Round Table and its associated committees as well as supporting pseudonymization and disclosure of data to the OHDP. As of April 1st, 2021, the Ministry views this initiative as operational and future governance is being determined within the scope of program oversight mode.

Ontario Health is working closely with the Ministry of Health and the ODHP program working groups to support and advise on the implementation of the platform. As part of its due diligence Ontario Health has completed a privacy impact assessment and a security threat risk assessment of the Ontario Health data environment.

**OLIS Lab Automation**

Ontario Health deployed the COVID-19 Lab Automation project designed to improve the overall COVID-19 testing workflow between a site performing the initial COVID-19 sample collection (an “Assessment Centre”) and the laboratory to which the sample is sent for processing. The results of this project standardized and automated sample workflow where possible, utilizing handheld scanners and user-friendly electronic forms to capture patient data and other requisition information in a uniform manner, enabling a consistent experience for Assessment Centres. The project includes the use of a traceable barcoded label for each sample, allow routing to the closest lab with capacity, and improve workflow, allowing improved reporting of COVID-19 results to health care providers, public health units, and patients.

The Ontario Health privacy and information security teams were engaged to build privacy and security controls into the design of this project, conducted privacy and security assessments, as well as worked on supporting the drafting of an agreement framework to govern the handling of personal health information by Ontario Health.
5. Privacy and Security by the Numbers: Key Metrics

The following key privacy and security metrics highlight some of the work accomplished by the Privacy Office and Information Security Office in 2020/21 and provides an indication of Ontario Health’s compliance with legislative and regulatory requirements as well as with its privacy and security policies and procedures.

Highlights of Privacy Metrics

In 2020/21, Ontario Health implemented an integrated process to manage Freedom of Information (FOI) requests that are received across the agency. Ontario Health continues to process and manage FOI requests within the legislated times set out under the Freedom of Information and Protection of Privacy Act or ‘FIPPA’.

<table>
<thead>
<tr>
<th>Freedom of Information Requests (FOI)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td><strong>FOI Requests Received</strong></td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td><strong>FOI Requests Completed</strong></td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td><strong>FOI Abandoned / Transferred</strong></td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>

Ontario Health manages, or has custody or control of, a large volume of records and data sets e.g. **85,450,000** patient records and delivers or supports the delivery of programs and services that entail millions of transactions e.g. Cancer Screening Program, Virtual Care. The metrics below include unintended breaches by health care providers and Ontario Health employees, and situations that once investigated were not considered a breach (‘incidents’). An example of a privacy breach is when an employee inadvertently accesses PHI where it is not required for the purposes of their job duties. Another example is when an external organization sends PHI to Ontario Health where Ontario Health did not request or need that information.

The volume of incidents and 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 alleged and actual privacy breaches and incidents are investigated by the Privacy Office in collaboration with the relevant stakeholders, with mitigating strategies and recommendations implemented to prevent future breaches and incidents from occurring.

<table>
<thead>
<tr>
<th>Privacy Breaches and Incidents (includes suspected breaches)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Breaches &amp; Incidents</strong></td>
</tr>
<tr>
<td>259</td>
</tr>
</tbody>
</table>

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

- Receives and implements requests from patients to place a consent directive on their records of PHI in the EHR; and
- Facilitates health information custodians in providing access to an individual for their records of PHI in the EHR, as well as to make corrections to these records where applicable.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Access &amp; Correction Requests</td>
<td>76</td>
<td>111</td>
<td>77</td>
<td>125</td>
</tr>
<tr>
<td>Consent Directive Requests</td>
<td>59</td>
<td>55</td>
<td>85</td>
<td>84</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Completed PIAs</td>
<td>48</td>
<td>42</td>
<td>48</td>
<td>22</td>
</tr>
</tbody>
</table>

**Highlights of Security Metrics**

The below security key metrics highlighting the number of completed internal and external Threat Risk Assessments (TRA), other types of requested security assessments, and penetration tests against new systems or changes to the operation. In addition, the below table indicates the total number of internal and external events and incidents such as phishing attacks, or any kind of indication of compromise (IOC) that needed investigation. Also, in order to be vigilant and compliant with the good industry practices and standards, the below number of full vulnerability scans were conducted on a monthly or quarterly base across different network infrastructures within Ontario Health.

<table>
<thead>
<tr>
<th>Key Cyber Security Activities - 2020-2021</th>
<th>TRA</th>
<th>Security Assessment</th>
<th>Penetration Test</th>
<th>Incident Assessed</th>
<th>Full Vulnerability Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completed Number of Assessments by Type</td>
<td>22</td>
<td>15</td>
<td>9</td>
<td>55</td>
<td>56</td>
</tr>
</tbody>
</table>
As with most government and private sector organizations, the provincial health care sector and its services are continuously under external attack from hackers from around the world. The main venue by which hackers attempt to reach and penetrate a company’s computing enterprise is the email. Below is a representation of the magnitude of email which traverses the provincial health care sector and the protection capabilities which have been put in place to defend against rogue malicious actors and eliminate malicious emails being delivered to end user mailboxes.

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

Continued Harmonization of Privacy and Security Program Activities and Supporting Policies
In alignment with the IPC’s recommendation that Ontario Health should amend its information practices to reflect the agency’s new governance and accountability framework, the privacy and security teams continue to work towards harmonized privacy and security programs that are supported through a common set of policies and procedures. Harmonized privacy and security programs will provide a more streamlined and clearer framework for Ontario Health employees to follow and understand when complying with their privacy and security responsibilities in their day-to-day work. It will also enable broader data sharing across the agency by ensuring a common, standard set of privacy and security controls across the agency, in compliance with new prescribed roles and the highest standard of requirements.

Privacy Operating Model
In October 2020 Ontario Health established its new organizational structure and operating model. With the new Ontario Health Legal, Privacy, Risk and Governance portfolio in place there is a need
to align and re-design people, processes and technology, that have transferred from each of the legacy organizations privacy teams, to set up the Privacy Office of the Legal, Privacy, Risk and Governance portfolio and Ontario Health for success.

Through transfers Ontario Health has assumed multiple roles under PHIPA. Through these prescribed roles, and other applicable legislative frameworks, Ontario Health has a complex compliance and agreement framework. As Ontario Health continues forming as a new organization, the Privacy Office is working to operationalize this new complex compliance framework and privacy program activities, in lock step with the cyber security and other business partners in a manner that is simple, effective and meaningful for Ontario Health staff and the health sector, while maximizing the value of resources. It is critical that the operating model allows Ontario Health to maintain trust, support provincial work and optimize the use of data for good as it continues transforming the health system, ensuring Ontarians receive the best possible care.

**Enabling use of data across Ontario Health**

Ontario Health holds key health system data assets which were transferred from Ontario’s legacy health system agencies pursuant to the Connecting Care Act. Currently, these data assets are managed in accordance to the legislative authorities assigned to each legacy agency. The privacy and Security team, working in close collaboration with Ontario Health’s Data Acquisition and Services Team, is working to optimize the use of these data assets to support Ontario Health’s mandate, including to support the agency’s role in pandemic planning.

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, 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 operating model.

**Health Care Navigation Service (HCNS)**

Health system navigation is a key challenge to address in Ontario’s health care system. While the government funds and oversees the delivery of a number of programs that are designed to help connect patients to health and social services, patients and caregivers are struggling to navigate Ontario’s health care system. The Ministry of Health is working on Health Care Navigation Services that will act as a one-stop ‘Digital Front Door’ to Ontario’s health care system, offering a place where all Ontarians can access health information, advice, and initial triage to become connected to publicly funded health care services across the province and to receive guidance throughout their health care journey. Ontario Health, including members of the Privacy Office, is supporting the Ministry of Health during the procurement phase, and will be managing the vendor agreement for the digital solution during planning and implementation. Ontario Health will act as the ministry’s PHIPA Agent for delivery of HCNS services. All permitted collections, uses, and disclosures of PHI will be specified in a PHIPA Agent agreement.
CHRIS Enhancements to Support Ontario Health Teams (OHTs)
The Client Health and Related Information System (CHRIS) is the home and community care electronic platform provided by Ontario Health. Ontario Health has engaged the North Toronto OHT to understand the data sharing needs of the OHTs to provide seamless and integrated healthcare to patients and how CHRIS can be enhanced to meet these requirements. To enable a new data sharing model that supports the OHTs, the Ontario Health Privacy Office has begun to review privacy controls and establish a supporting agreement structure.

Provincial Scale Virtual Solution for Substance Use Disorder (SUD)
At least 1 in 5 Canadians will experience a problem with substance use problem over their lifetime. This new project will collaborate with external groups towards the development of a SUD provincial virtual solution procurement and implementation as well as pre and post evaluation. Ontario Health will receive funding from the Ministry of Health and enter into a statement of work acting as coordinator of licenses on behalf of the province. Ontario Health will lead an external working group of stakeholders to develop a provincial implementation model to address regions in Ontario most impacted by COVID-19 where there has been suspension or modification to addiction services.

Continued Support for the Provincial Cyber Security Model
Ontario Health will continue to champion a provincial approach to Cyber Security, with the support of key stakeholders including, the Ministry of Health, Ministry of Government and Consumer Services, partner hospitals, and the broader public sector as they adopt the model and a collective defense of Ontario’s digital assets. This work will be accomplished through activities in Ontario Health’s Annual Business Plan, as well as through opportunities that arise throughout the fiscal year.

Continued Enhancement of Ontario Health Cyber Security Controls
With the ever-changing risk environment and the particular focus of cyber-attacks upon the health care sector, Ontario Health will continue to invest and improve the maturity of its cyber security control suite. This will establish safe and effective operation of Ontario Health systems and support the compliance and assurance expected of Ontario Health as a byproduct of good cyber security practices.