Exhibit "B"

OH Prescribed Organization - Privacy, Security, Human Resources and Organizational Indicator Report

Indicators below are provided for Ontario Health (**OH**) as a Prescribed Organization, in relation to the Electronic Health Record (**EHR**), for the time period of **June 1, 2021, to August 2, 2022**, unless otherwise specified.

Part 1 – Privacy Indicators

General Privacy Policies, Procedures & Practice

Policies - Privacy Indicator	Assessment
The dates privacy policies and procedures were reviewed since the prior review by the IPC	All general privacy policies, procedures and practices were reviewed by OH and the Information and Privacy Commissioner (**IPC**) during the prior review by IPC that was completed on October 1, 2021. No further reviews of these privacy policies, procedures and practices have occurred, and no amendments have been made since the prior review by the IPC. The EHR Consent Directive Request Form is currently under review. See **Appendix A** for a list of general privacy policies, procedures and practices that apply to OH.
Whether amendments were made to existing privacy policies and procedures as a result of the review, and if so, a list of the amended privacy policies and procedures and, for each policy and procedure amended, a brief description of the amendments made.	
Whether new privacy policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.	
The date each amended, and newly developed privacy policy and procedure was communicated to employees or other persons acting on behalf of the prescribed organization and, for each amended and newly developed privacy policy and procedure communicated to employees or other persons acting on behalf of the prescribed organization, the nature of the communication.	
Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.	

Receiving Personal Health Information

Receiving PHI - Privacy Indicator	Assessment
The number of repositories of personal health information that are accessible by means of the electronic health record.	6
The number of descriptions of types of personal health information received by the prescribed organization for the purpose of creating or maintaining the electronic health record.	6

Receiving PHI - Privacy Indicator	Assessment
The number of descriptions of types of personal health information received by the prescribed organization for the purpose of creating or maintaining the electronic health record that were reviewed since the prior review by the IPC.	6
Whether amendments were made to existing descriptions of types of personal health information as a result of the review, and if so, for each description amended, a brief explanation of the amendments made.	No amendments have been made to the descriptions of types of personal health information (**PHI**).

Managing Consent in the Electronic Health Record

Consent - Privacy Indicator	Assessment
The number of instances in which a consent directive has been made, modified or withdrawn since the prior review by the IPC.	2,247
The number of instances in which a notice of a consent directive has been provided to a health information custodian in accordance with subsection 55.6 (7) of the Act since the prior review by the IPC.	Where a health information custodian (**HIC**) attempts to access PHI in the EHR that is subject to a consent directive, OH provides notice to the HIC through an electronic alert. OH does not maintain a record of the number of electronic alerts of consent directives issued in respect of the EHR (except for those that result in a consent directive override). However, OH has reasonable controls in place to ensure that the electronic alerts continue to function properly. This process is further documented in the OH PO Statement of Requested Exceptions.
The number of instances in which a health information custodian has overridden a consent directive pursuant to section 55.7 of the Act since the prior review by the IPC and the number of occasions on which each of subsection 55.7(1), (2) or (3) of the Act was invoked to override the consent directive.	Total: 5,392 • Reason 1 (express consent): 5,094 • Reasons 2 & 3 (significant risk of bodily harm – self or others): 298* *The 298consent overrides relate to overrides conducted in respect of the Acute and Community Clinical Data Repository (**acCDR**) (there were no overrides conducted for reasons 2 and 3 in respect of the other EHR repositories). Currently, OH's log of consent directives does not differentiate between reasons 2 and 3 where the consent directive is performed in the acCDR.

Consent - Privacy Indicator	Assessment
The number of instances in which a notice of a consent override has been provided to a health information custodian in accordance with subsection 55.7(6) of the Act since the prior review by the IPC.	Of the 5,392 instances in which a HIC has overridden consent in accordance with s. 55.7 of PHIPA since the prior review by the IPC, 5,386[1] notices have been provided to the relevant HIC in accordance with s.55.7(6) for June 1, 2021, to August 2, 2022.
The dates on which reports of consent overrides were made to the IPC pursuant to paragraph 16 of section 55.3 of the Act since the prior review by the IPC.	1 report was provided to the IPC as part of the IPC's initial review of the Prescribed Organization that was completed on October 1, 2022.
The number of requests received from health information custodians pursuant to paragraph 9 of section 55.3 of the Act for the electronic records of consent directives and consent overrides since the prior review by the IPC.	3
The number of requests received from the IPC pursuant to paragraph 8 of section 55.3 for the electronic records of consent directives and consent overrides since the prior review by the IPC.	0

Viewing, Handling or Otherwise Dealing with Personal Health Information

Approval to Use PHI - Privacy Indicator	Assessment
The number of employees or other persons acting on behalf of the prescribed organization granted approval to view, handle or otherwise deal with personal health information.	a. Application access – 60 OH agents b. Operational access – 153 OH agents Application access includes access provisioned directly to the EHR application that hosts records of PHI. Operational access includes access provisioned for maintenance and monitoring of the back-end systems that host the EHR applications, where there is potential exposure to PHI.

[1] Updated on October 12, 2023

Provision of Personal Health Information Pursuant to Minister's Direction

Provision PHI - Privacy Indicator	Assessment
The number of directions issued by the Minister pursuant to subsection 55.9(8) of the Act requiring the prescribed organization to provide to the Minister personal health information that is accessible by means of the electronic health record since the prior review by the IPC.	0
The number of directions issued by the Minister requiring the prescribed organization to provide personal health information that is accessible by means of the electronic health record to a person for the purposes of subsection 55.10(1) of the Act since the prior review by the IPC.	0
The number of directions issued by the Minister requiring the prescribed organization to provide personal health information that is accessible by means of the electronic health record to a prescribed person for the purposes of clause 39(1)(c) of the Act since the prior review by the IPC.	0
The number of directions issued by the Minister requiring the prescribed organization to provide personal health information that is accessible by means of the electronic health record to a person for the purposes of subsection 39(2) of the Act since the prior review by the IPC.	0
The number of directions issued by the Minister requiring the prescribed organization to provide personal health information that is accessible by means of the electronic health record to a researcher for the purposes of section 44 of the Act since the prior review by the IPC.	0
The number of directions issued by the Minister requiring the prescribed organization to provide personal health information that is accessible by means of the electronic health record to a prescribed entity for the purposes of section 45 of the Act since the prior review by the IPC.	0

Access and Correction

Access & Correction - Privacy Indicator	Assessment
The number of requests made by individuals to access records of personal health information that are accessible by means of the electronic health record since the prior review by the IPC. • The number of requests made by individuals to correct records of personal health information that are accessible by means of the electronic health record since the prior review by the IPC. • The number of refusals under the Act of a request for access to a record, the provisions of the Act under which access was refused and the number of occasions on which each provision was invoked. • The number of refusals under the Act of a request to correct a record, the provisions of the Act under which the correction was refused and the number of occasions on which each provision was invoked. • The amount of fees collected by the prescribed organization under subsection 54 (10) of the Act, if any.	As section 51(5) of Part V of the Personal Health Information Protection Act, (PHIPA) has not yet been proclaimed, no access and correction decisions have been made by OH in its capacity as a Prescribed Organization. OH facilitates access and correction requests as an Agent of Health Information Custodians (HIC(s)) by identifying responsive records and providing them directly to the responsible HIC for fulfilling their obligations under Part V of the PHIPA. OH does not release records directly to the requester nor make any access/correction decisions under the PHIPA. The reporting obligations to the IPC related to these access and correction requests would rest with HICs that are public sector institutions as part of their annual statistical reporting.

Agreements with Third-Party Service Providers

Agreements - Privacy Indicator	Assessment
Number of agreements executed with third party service providers with access to personal health information since the prior review by the IPC	1 new agreement has been executed with third party service providers for which access to PHI is expected to be provided. *Does not include renewal of existing agreements

Privacy Impact Assessments

PIA - Privacy Indicator	Assessment
The number and a list of privacy impact assessments completed since the prior review by the IPC and for each privacy impact assessment: • A description of the existing or proposed system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record or the types of personal health information that will be provided to the prescribed organization for the purposes of developing or maintaining the electronic health record, as the case may be; • For each system that retrieves or will retrieve, process, or integrate personal health information, a description of the types of personal health information that is or will be retrieved, processed, or integrated; • The date of completion of the privacy impact assessment; • A brief description of each recommendation; • The date each recommendation was addressed or is proposed to be addressed; and • The manner in which each recommendation was addressed or is proposed to be addressed.	Total number:10 See **Appendix B** for details

PIA - Privacy Indicator	Assessment
The number and a list of privacy impact assessments undertaken but not completed since the prior review by the IPC and the proposed date of completion	Total number: 8 • Ontario Laboratories Information System (**OLIS**) Technology Upgrade. Project not yet completed; estimated go-live September 2022. Privacy impact assessments (**PIA**) to be completed prior to go-live. • Enhanced Database Security Monitoring. Project was cancelled, so as a result while a PIA was started, it will not be completed. • Health Information Access Layer (**HIAL**) Consolidation 2: Workstream 6. Project not yet completed; estimated go-live September 2022. PIA to be completed prior to go-live. • Renal Dialysis Information System (**RDIS**) Integration with OLIS. Project not yet completed; estimated go-live October 2022. PIA to be completed prior to go-live. • Individual Access to the EHR. Project not yet completed; estimated go-live September 2022. PIA to be completed prior to go-live. • Clinical Support Systems (**CSS**). Project not yet completed; estimated go-live September 2022. PIA to be completed prior to go-live. • Connecting Ontario Release 2 (10.8). Project not yet completed; estimated go-live October 2022. PIA to be completed prior to go-live. • Southlake Dr. First Solution. Project not yet completed; estimated go-live October 2022. PIA to be completed prior to go-live.
The number and a list of privacy impact assessments that were not undertaken but for which privacy impact assessments will be completed and the proposed date of completion	Total number: 2 • ConnectingOntario Release 12. Project not yet completed; PIA to be completed prior to go-live (March 2023) • Comprehensive Medication Record for Ontarians (**CMRO**). Project not yet completed; PIA to be completed prior to go-live (Feb 2024)
The number of determinations made since the prior review by the IPC that a privacy impact assessment is not required and, for each determination, the existing or proposed system that retrieves, processes, or integrates personal health information, and a description of the types of personal health information that is or will be retrieved, processed or integrated that is at issue, and a brief description of the reasons for the determination.	Total number: 0 • No determinations were made since the prior review by the IPC that a privacy impact assessment is not required.

PIA - Privacy Indicator	Assessment
The number and a list of privacy impact assessments reviewed since the prior review by the IPC and a brief description of any amendments made.	Total number: 0 • No PIAs were reviewed or refreshed

Privacy Audit Program

Audit - Privacy Indicator	Assessment
For the electronic records the prescribed organization is required to keep pursuant to paragraphs 5 and 6 of section 55.3 and to audit and monitor pursuant to paragraph 7 of section 55.3, since the prior review by the IPC: • The number of audits conducted or the frequency with which the • audits have been conducted; • The nature and scope of each audit conducted; • The date of completion of the audit; • A brief description of each recommendation made; • The date each recommendation was addressed or is proposed to be addressed; and • The manner in which each recommendation was addressed or is proposed to be addressed.	OH continuously monitors all electronic records (audit events) that OH is required to maintain in relation to consent directives and consent overrides through information and event monitoring applications. OH conducts audits of the electronic records that OH is required to maintain in relation to consent directives and overrides if: • There is an alert generated through the information and event monitoring systems that has been reviewed and requires investigation (i.e. constitutes a privacy incident/suspected breach); • If there is a privacy incident, risk or complaint identified or raised in relation to a consent directive or override; or • If there is an audit scheduled in accordance with OH's Privacy Audit and Compliance Policy, and the Privacy Audit Schedule, to assess compliance with OH's privacy policies, procedures, and practices, that requires review of these electronic records. One audit of electronic records of consent directive override is currently in process to assess compliance with OH's privacy policies, procedures, and practices. This audit is expected to be complete by December 31st, 2022. Recommendations will be formalized once the audit is complete.

Audit - Privacy Indicator	Assessment
The dates of audits of employees and other persons acting on behalf of the prescribed organization granted approval to view, handle or otherwise deal with personal health information since the prior review by the IPC and for each audit conducted: • The date of completion of the audit; • A brief description of each recommendation made; • The date each recommendation was addressed or is proposed to be addressed; and • The manner in which each recommendation was addressed or is proposed to be addressed.	See **Appendix C** details.
The number and a list of audits completed to assess compliance with the privacy policies, procedures and practices put in place by the prescribed organization completed since the prior review by the IPC and for each audit: • The date of completion of the audit; • A brief description of each recommendation made; • The date each recommendation was addressed or is proposed to be addressed; and • The manner in which each recommendation was addressed or proposed to be addressed.	Total Audits: 2 See **Appendix C** details.
The number and a list of all other privacy audits completed since the prior review by the IPC and for each audit: • A description of the nature and type of audit conducted; • The date of completion of the audit; • A brief description of each recommendation made; • The date each recommendation was addressed or is proposed to be addressed; and • The manner in which each recommendation was addressed or is proposed to be addressed.	No other privacy audits were conducted since the prior review of the IPC, in respect of the EHR.

Privacy Breaches

Privacy Indicator	Assessment
The number of notifications of privacy breaches or suspected privacy breaches received by the prescribed organization since the prior review by the IPC.	27
The number of privacy breaches identified by the prescribed organization since the prior review by the IPC.	23
The number of privacy breaches caused by one or more health information custodians.	19 Actual/Confirmed breaches: 17 Suspected breaches: 2 Policy Breaches[2]: 0
The number of privacy breaches caused by the prescribed organization or a system that retrieves, processes, or integrates personal health information in the electronic health record.	Actual/Confirmed breaches: 4 Suspected breaches: 0 Policy Breaches: 0
The number of privacy breaches caused by a person who is not an employee or other person acting on behalf of the prescribed organization or an agent or electronic service provider of a health information custodian.	0

[2] Note: Policy breaches are a sub-type of privacy breaches for the purpose of complying with the Manual for the Review and Approval of Prescribed Organization.

Privacy Indicator	Assessment
With respect to each privacy breach caused by the prescribed organization; a system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record; or a person who is not an employee or other person acting on behalf of the prescribed organization or an agent or electronic service provider of a health information custodian since the prior review by the IPC: • Whether the privacy breach or suspected privacy breach was caused by the prescribed organization; • Whether the privacy breach or suspected privacy breach was caused by a system that retrieves, processes, or integrates personal health information that is accessible by means of the electronic health record; • Whether the privacy breach or suspected privacy breach was caused by a person who is not an employee or other person acting on behalf of the prescribed organization or an agent or electronic service provider of a health information custodian; • The nature and scope of the privacy breach; • The cause of the privacy breach; • The date that senior management of the prescribed organization was notified; • The containment measures implemented; • The date(s) that the containment measures were implemented; • The date(s) that notification was provided to the health information custodians or any other organizations; • The date that the investigation was commenced; • The date that the investigation was completed; • A brief description of each recommendation made; • The date each recommendation was addressed or is proposed to be addressed; and • The manner in which each recommendation was addressed or is proposed to be addressed.	See **Appendix D** for details.

Privacy Complaints

Privacy Indicator	Assessment
The number of privacy complaints received since the prior review by the IPC.	1
Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the IPC and with respect to each privacy complaint investigated: • The date the privacy complaint was received; • The nature of the privacy complaint; • The date the investigation was commenced; • The date of the written communication to the individual made the privacy complaint in relation to the commencement investigation; • The date that the investigation was completed; • A brief description of each recommendation made; • The date each recommendation was addressed, or is proposed to be, addressed; • The manner in which each recommendation was addressed, or is proposed to be, addressed; and • The date of written communication to the individual who made the privacy complaint describing the nature and findings of the investigation and the measures taken in response to the complaint.	1 N/A - No OH related complaints. The 1 complaint is regarding a Health Information Custodian (HIC) and was forwarded to the HIC for investigation.
Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the IPC and with respect to each privacy complaint not investigated: • The date that the privacy complaint received; • The nature of the complaint; and • The date of the written communication to the individual who made the privacy complaint and a brief description of the content of the letter.	0

Part 2 – Security Indicators

General Security Policies and Procedures

Security Indicator	Assessment
The dates that the security policies and procedures were reviewed since the prior review by the IPC	See **Appendix F** for details
Whether amendments were made to existing security policies and procedures as a result of the review, and if so, a list of the amended security policies and procedures and, for each policy and procedure amended, a brief description of the amendments made.	
Whether new security policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.	
The dates that each amended, and newly developed security policy and procedure was communicated to employees and other persons acting on behalf of the prescribed organization and, for each amended and newly developed security policy and procedure communicated to employees and other persons acting on behalf of the prescribed organization, the nature of the communication.	
Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.	

Physical Security

Security Indicator	Assessment
Dates of audits of employees and other persons acting on behalf of the prescribed organization granted approval to access the premises and locations within the premises where records of personal health information are retained since the prior review by the IPC, and for each audit: • A brief description of each recommendation made; • The date each recommendation was addressed or is proposed to be addressed; and • The manner in which each recommendation was, or is proposed to be, addressed.	Regular audits are performed to review access card permissions to ensure those agents who have been granted approval to access the OH premises, including access to premises with PHI. These audits took place on: • August 2021 • February 2022 • June 2022 No recommendations were made.

Acceptable Use Agreements

Security Indicator	Assessment
The number of Acceptable Use Agreements acknowledged and agreed to by employees or other persons acting on behalf of the prescribed organization since the prior review by the IPC.	OH is in the process of deploying the Acceptable Use Agreement to all employees and other persons acting on behalf of OH. Since the last review, as of June 12, 2022, 2828 employees and other persons acting on behalf of OH have acknowledged and agreed to the terms of the Acceptable Use Agreement.

End User Agreements

Security Indicator	Assessment
The number of End User Agreements acknowledged and agreed to by end users who provide personal health information to or collect personal health information by means of the electronic health record.	OH does not enter into End User Agreements directly with each end-user who accesses PHI from or provides PHI to the EHR.OH enters into agreements with each HIC that collects PHI from and provides PHI to the EHR. These agreements include provisions related to compliance of the HIC's end-users. In addition, OH is working to address the end-user agreements recommendation issued to Ontario Health as set out in the IPC's approval letter, dated October 1, 2021, re: *Initial Review of the Practices and Procedures of Ontario Health as a Prescribed Organization under the Personal Health Information Protection Act, 2004.*This approach is further identified in the OH PO Statement of Requested Exceptions.

Security Audit Program

Security Indicator	Assessment
The number of requests received from health information custodians pursuant to paragraph 9 of section 55.3 for the electronic records that the prescribed organization is required to keep pursuant to paragraph 4 of section 55.3 of the Act, since the prior review by the IPC.	384
The number of requests received from the IPC pursuant to paragraph 8 of section 55.3 for the electronic records that the prescribed organization is required to keep pursuant to paragraph 4 of section 55.3 of the Act, since the prior review by the IPC.	0

Security Indicator	Assessment
For the electronic records the prescribed organization is required to keep pursuant to paragraph 4 of section 55.3 and to audit and monitor pursuant to paragraph 7 of section 55.3 of the Act, since the prior review by the IPC: • The number of audits conducted or the frequency with which the audits have been conducted; • The nature and scope of each audit conducted; • The date of completion of the audit; • A brief description of each recommendation made; • The date each recommendation was addressed or is proposed to be addressed; and • The manner in which each recommendation was addressed or is proposed to be addressed.	OH continually audits and monitors all electronic records that OH is required to keep under paragraph 4 of section 55.3, through auditing and event monitoring tools. These tools, including security information and event monitoring (**SIEM**) software, and the monitoring control technology application, monitor and analyze events such as those related to application logins and access to PHI. These auditing and monitoring tools produce alerts and reports based on defined use cases or parameters (e.g. large volume of access to PHI over short period of time) that are reviewed by OH's privacy and security teams or the health information custodian whose agents performed the access subject to the report or alert, as applicable. If, upon review of the alert or report, a privacy or security incident is detected, it is managed in accordance with the OH Privacy Incident Management Policy and Procedure, EHR Privacy Incident Management Policy and Procedure and/or Information Security Incident Management Standard. Any related recommendations that arise from the management of privacy and security incidents (including auditing and monitoring) are included in the privacy and/or security incident logs (see Privacy Breaches section of indicators and the Information Security Breaches indicator section below).
The dates of the review of all other system control and audit logs since the prior review by the IPC and a general description of the findings, if any, arising from the review of system control and audit logs.	OH continually monitors our system control and audit logs using a number of automated systems. These systems monitor for errors in applications, availability of system components, and security events. These logs are reviewed both through automated means, as well as by OH operations staff.

Security Indicator	Assessment
The number and a list of all other security audits completed since the prior review by the IPC and for each audit: • A description of the nature and type of audit conducted; • The date of completion of the audit; • A brief description of each recommendation made; • The date that each recommendation was addressed or is proposed to be addressed; and • The manner in which each recommendation was addressed or is expected to be addressed.	Total Security Audits: 7 See **Appendix G** for details.

Threat and Risk Assessments

Security Indicator	Assessment
The date of all threat and risk assessments that have been completed since the prior review by the IPC and for each threat and risk assessment: • The system that is at issue; • The date the threat and risk assessment was completed or is expected to be completed; • A brief description of the recommendations arising from the threat and risk assessment; • The date each recommendation was or is expected to be addressed; and • The manner in which each recommendation was or is expected to be addressed.	Total TRAs: 2 See **Appendix G** for details.

Information Security Breaches

Security Indicator	Assessment
The number of notifications of security breaches or suspected security breaches received by the prescribed organization since the prior review by the IPC.	Total security breaches impacting EHR: 0 Total suspected security breaches: 11 Ten of the suspected security breaches were breaches at HICs, investigated by OH to determine whether a subsequent breach of the EHR occurred.

Security Indicator	Assessment
The number of security breaches identified since the prior review by the IPC.	0
The number of security breaches caused by one or more health information custodians.	0
The number of security breaches caused by the prescribed organization or a system that retrieves, processes, or integrates personal health information in the electronic health record.	0
The number of security breaches caused by a person who is not an employee or other person acting on behalf of the prescribed organization or an agent or electronic service provider of a health information custodian.	0
With respect to each security breach or suspected security breach caused by the prescribed organization; a system that retrieves, processes or integrates personal health information in the electronic health record; or a person who is not an employee or other person acting on behalf of the prescribed organization or an agent or electronic service provider of a health information custodian since the prior review by the IPC: • Whether the security breach or suspected security breach was caused by the prescribed organization; • Whether the security breach or suspected privacy breach was caused by a system that retrieves, processes or integrates personal health information in the electronic health record; • Whether the security breach or suspected security breach was caused by a person who is not an employee or other person acting on behalf of the prescribed organization or an agent or electronic service provider of as health information custodian; • The nature and scope of the security breach; • The cause of the security breach; • The date that senior management of the prescribed organization was notified; • The containment measures implemented; • The date(s) that the containment measures were implemented; • The date(s) that notification was provided to the health information custodians or any other organizations; • The date that the investigation was commenced; • The date that the investigation was completed; • A brief description of each recommendation made; • The date each recommendation was addressed or is proposed to be addressed; and • The manner in which each recommendation was addressed or is proposed to be addressed.	There has been one (1) suspected security breach (policy violation) of the EHR caused by the Prescribed Organization. See **Appendix H** for details.

Part 3 – Human Resources Indicators

Privacy Training & Awareness

Human Resources Indicator	Assessment
The number of employees or other persons acting on behalf of the prescribed organization who have received and who have not received initial privacy training since the prior review by the IPC.	Received initial, role based EHR privacy training: 63 Not received initial, role based EHR privacy training: 0
The date of commencement of the employment, contractual or other relationship for employees and other persons acting on behalf of the prescribed organization who have yet to receive initial privacy training and the scheduled date of the initial privacy training.	N/A - 0 employees and other OH agents who have access to PHI that is accessible via the EHR have yet to take their initial/role based EHR privacy training since the prior review by the IPC.
The number of employees or other persons acting on behalf of the prescribed organization who have attended and who have not attended ongoing privacy training each year since the prior review by the IPC.	2022 Annual Training* Attended: 2814 Not Attended: 4** *This indicator does not include employees and other OH agents from the Patient Ombudsman Office who received separate privacy training specific to the Patient Ombudsman's Office. These agents are not granted approval to access PHI that is available through the EHR. **The 4 agents who have not completed the training do not have access to PHI in their capacity as an Agent of OH.
The dates and number of communications to agents by the prescribed organization in relation to privacy since the prior review by the IPC and a brief description of each communication.	See **Appendix I** for details

Security Training & Awareness

Human Resources Indicator	Assessment
The number of employees or other persons acting on behalf of the prescribed organization who have received and who have not received initial security training since the prior review by the IPC.	63 employees and other OH agents completed EHR initial/role-based security training since the prior review by the IPC. 0 employees and other OH agents who may access PHI that is accessible via the EHR, have yet to take their initial/role based EHR security training since the prior review by the IPC.
The date of commencement of the employment, contractual or other relationship for employees and other persons acting on behalf of the prescribed organization who have yet to receive initial security training and the scheduled date of the initial security training.	N/A - 0 employees and other OH agents acting on behalf of OH who may access PHI that is accessible via the EHR, have yet to take their initial/role based EHR security training since the prior review by the IPC.
The number of employees or other persons acting on behalf of the prescribed organization who have attended and who have not attended ongoing privacy training each year since the prior review by the IPC.	2022 Security Training: Attended: 2886 Not Attended: 4* *The 4 agents who have not completed the training do not have access to PHI in their capacity as an Agent of OH.
The dates and number of communications to agents by the prescribed organization in relation to security since the prior review by the IPC and a brief description of each communication.	See **Appendix I** for details.

Confidentiality Agreements

Human Resources Indicator	Assessment
The number of employees or other persons acting on behalf of the prescribed organization who have executed and who have not executed Confidentiality Agreements each year since the prior review by the IPC.	In 2022, 2893 individuals have signed a confidentiality agreement. No individuals have yet to sign a confidentiality agreement.
The date of commencement of the employment, contractual or other relationship for employees or other persons acting on behalf of the prescribed organization who have yet to execute the Confidentiality Agreement and the date by which the Confidentiality Agreement must be executed.	N/A – not individuals have yet to execute an OH confidentiality agreement.

Termination or Cessation

Human Resources Indicator	Assessment
The number of notifications received from employees or other persons acting on behalf of the prescribed organization since the prior review by the IPC related to termination of their employment, contractual or other relationship with the prescribed organization.	OH has received 553 notifications from OH agents since the last review related to termination of their employment, contractual or other relationship with OH.

Part 4 – Organizational Indicators

Risk Management

Organizational Indicator	Assessment

The dates that the corporate risk register was reviewed by the prescribed organization since the prior review by the IPC.	The corporate risk register was reviewed by OH on the following dates, and the corresponding amendments were made:
	• 2021-06-05
	  ○ Consolidated ministry and board risk registers from Q4 FY20/21, and entered quarterly updates to all enterprise risks for Q1 FY21/22
	• 2021-09-13
	  ○ Quarterly update for Q2 FY21/22
	• 2021-11-08
	  ○ Minor updates to Q2 FY21/22 risks
	• 2021-12-18
	  ○ Consolidated template updates from Ministry Q3 risk reporting template and Board feedback on risk definitions; Quarterly update for Q3 FY21/22
	• 2022-02-10
	  ○ Minor updates for Board Q3 FY21/22 risk report
	• 2022-04-11
	  ○ Quarterly update for Q4 FY21/22
	• 2022-05-10
	  ○ Minor updates for Board Q4 FY21/22 risk report

Whether amendments were made to the corporate risk register as a result of the review, and if so, a brief description of the amendments made.	

Business Continuity & Disaster Recovery

Organizational Indicator	Assessment
The dates that the business continuity and disaster recovery plan was tested since the prior review by the IPC.	**Disaster Recovery:** The OH Disaster Recovery Plan is tested annually via table-top exercise, which was conducted on December 6, 2021, and March 1, 2022. On a daily basis, OH validates all previous day's backups that were successfully completed, including the Digital Health Drug Repository (DHDR), Primary Care Clinical Data Repository (pcCDR), Ontario Laboratory information System (OLIS), and Diagnostic Imaging Common Service (DI CS) systems. **Business Continuity Plan:** The Technology Continuity Planning (TCP) team holds yearly mini tabletop tests with relevant departments: Dates of tests with name of department: • April 5th, 2022 Cyber Security Defense • April 7th, 2022 Platform & Cloud Operations • April 7th, 2022 IT Service Management • April 12th, 2022 Tech Planning Continuity • April 22th, 2022 Product Mgmt & Customer Value • April 13th, 2022 Cyber Security Governance • April 13th, 2022 Product Management Delivery • March 29th, 2022 Product Mgmt & Cust Value • March 10th, 2022 Project Governance • March 7th, 2022 Product Mgmt & Cust Value & Products • March 24th, 2022 Product Mgmt & Cust Value & Products (Client Integration) • March 9th, 2022 Data Centre Services • March 15th, 2022 Digital Health Standards • March 17th, 2022 Digital Strategy Management • March 24th ,2022 Product Mgmt & Customer Value • March 8th, 2022 Product Mgmt & Cust Value & Products • March 8th, 2022 Customer Experience • March 4th, 2022 Customer Experience & Business • March 15th, 2022 Cloud Centre of Excellence • March 17th, 2022 Architecture Program • March 22nd, 2022 Network Services • March 16th, 2022 Transformation Centre of Excellence • March 25th, 2022 Connected Health Programs • March 18th, 2022 Enterprise Products • March 16th, 2022 Customer Transition

Organizational Indicator	Assessment
Whether amendments were made to the business continuity and disaster recovery plan as a result of the testing, and if so, a brief description of the amendments made.	**Disaster Recovery:** Updates have been made related to One ID, the application/infrastructure dependency matrix within the Guelph Data Centre (GDC). **Business Continuity Plan:** Due to the amalgamation of legacy health agencies into Ontario Health, several changes are being made to the Business Continuity Plan as functions move between departments and get updated. Details on specific changes may be found in See details I **Appendix J** - Business Continuity & Disaster Recovery Table-top Testing Log.

Appendix A – General Privacy Policies, Procedures & Practice

Name of Policy or Document	Review Period	Approval Date
EHR Plain Language Description and List of EHR Repositories	June 2021	June 2021
EHR Policy for Receiving PHI	June 2021	November 11, 2021
EHR Privacy Incident Management Policy and Procedure	June 2021	November 11, 2021
EHR Inquiries and Compliant policy and Procedure	June 2021	November 11, 2021
EHR Request for Access to PHI Policy and Procedure	July 2021	November 11, 2021
EHR Request for Correction to PHI Policy and Procedure	July 2021	November 11, 2021
EHR Retention Policy and Procedure	June 2021	November 11, 2021
EHR Statement of Information Practices	June 2021	June 2021
EHR Consent Directive and Consent Override Policy	August 2021	November 11, 2021
PIA Standard	June 2021	November 11, 2021
Privacy Governance and Accountability Framework	June 2021	June 2021
Privacy Audit & Compliance Policy	June 2021	November 11, 2021
Privacy Complaints and Inquiries Policy and Procedure	June 2021	November 11, 2021
Privacy Incident Management Policy and Procedure	June 2021	November 11, 2021
Privacy Policy	August 2021	September 23, 2021
Privacy Transparency Policy	June 2021	November 11, 2021
Privacy Use and Disclosure Policy	August 2021	November 11, 2021
EHR Policy and Procedure for Agreements with Health Information Custodians and Coroners	April 2021	November 11, 2021
EHR Privacy Auditing and Monitoring Policy	July 2021	November 11, 2021
Privacy Notices Policy and Procedure	April 2021	November 11, 2021
Privacy and Security Log of Recommendations Standard	August 2021	September 15, 2021
Privacy and Security Training and Awareness Policy	Q1-Q2, 2021/22	November 11, 2021
Privacy Program Advisory Committee – Terms of Reference	June 2021	June 2021
Privacy Risk Management Policy	August 2021	November 11, 2021

Appendix B – Privacy Impact Assessment Log

PIA ID	Name of the Reviewed Existing or Proposed System & Type of Assessment	Type(s) of PHI retrieved, processed, or integrated	Date PIA completed (YYYY-MM-DD)	Summary of Residual Risk Description	Recommendation ID & Summary of Recommendations	Date recommendation was addressed or expected to be addressed. (YYYY-MM-DD)	The manner each recommendation was or is expected to be addressed	Status
PIA-0076 – WS2	Health Integration Access Layer (**HIAL**) Consolidation – Workstream 2 PTA	DHDR and acute and community Clinical Data Repository (CDR)	2021-09-24	No risks identified.	There were no recommendations made.	N/A	N/A	Closed
PIA-0076 – WS7	Health Integration Access Layer (**HIAL**) Consolidation – Workstream 7 PTA	PCR	2022-02-11	No risks identified.	There were no recommendations made.	N/A	N/A	Closed
PIA-0076 – WS8	Health Integration Access Layer (**HIAL**) Consolidation – Workstream 8 PTA	PCR	2021-11-21	No risks identified.	There were no recommendations made.	N/A	N/A	Closed
PIA-0078	CMTA Currency Upgrade PTA	All EHR repositories	2021-11-29	No risks identified.	There were no recommendations made.	N/A	N/A	Closed

PIA ID	Name of the Reviewed Existing or Proposed System & Type of Assessment	Type(s) of PHI retrieved, processed, or integrated	Date PIA completed (YYYY-MM-DD)	Summary of Residual Risk Description	Recommendation ID & Summary of Recommendations	Date recommendation was addressed or expected to be addressed. (YYYY-MM-DD)	The manner each recommendation was or is expected to be addressed	Status
PIA-0081	Point Click Care Integration with OLIS and DHDR PTA	OLIS and DHDR	2021-12-09	Closed in the course of the privacy assessment. No resulting risks.	**PIA-0081-01**: It was identified that the workflow is dependent on eConnect, and as such there was a risk of only partial data being accessible to PCC users if eConnect is removed from the workflow in future. As such, there is an agreed-to condition between PCC and OH that eConnect cannot be removed from the workflow; this condition resulted in a conditional pass on conformance testing and the conformance testing certificate documents the requirement to leverage eConnect. Further, as per the EHR Interface Service schedule, any significant future changes or enhancements (which would include the removal of eConnect from this workflow) will require that full conformance testing be undertaken and passed.	N/A	Closed in the course of the privacy assessment. At the time of a more robust integration, completion of full standard conformance testing is required.	Closed
				While the privacy assessment of this initiative determined that it conformed to existing approved models of OLIS and DHDR data provision, the condensed privacy review timeline was identified as a potential risk.	N/A - see associated 'summary of risk description'	N/A	Risk acceptance by OH. The OH Chief Privacy Officer (CPO) and Initiative Sponsor reviewed and approved this privacy assessment including this identified residual privacy risk.	Closed
PIA-0085 – R1	Connecting Ontario Release 10.8.1A PTA	All EHR repositories; however no PHI was used in the course of this initiative.	2021-10-27	No risks identified.	There were no recommendations made.	N/A	N/A	Closed
PIA-0092	OLIS Release 5 (5.1 and 5.2) PTA	OLIS	2021-12-15	No risks identified.	There were no recommendations made.	N/A	N/A	Closed

PIA ID	Name of the Reviewed Existing or Proposed System & Type of Assessment	Type(s) of PHI retrieved, processed, or integrated	Date PIA completed (YYYY-MM-DD)	Summary of Residual Risk Description	Recommendation ID & Summary of Recommendations	Date recommendation was addressed or expected to be addressed. (YYYY-MM-DD)	The manner each recommendation was or is expected to be addressed	Status
PIA-0093	HIS-OLIS Direct Integration PIA	OLIS; potentially all EHR repositories	2022-06-02	Risk #1 – Certain current-use hospital information system (HIS) solutions may not be able to provide the Hands-On-Keyboard (individual end-user) user data directly to OH in the transaction and as per the message specification. This risk is resulting from external HIS vendor and data specification standard challenges. Note, however, that in such cases this 'Hands-On-Keyboard' end user information remains present, captured, and stored by the HIC's HIS.	**PIA-0093-01**: Develop a time-limited exception that requires a reporting framework in order to permit applicable HIC HIS solutions to cause transactions via applicable EHR integrations. These transactions must meet the requirements of PHIPA 55.3(4ii) and applicable HICs are required to store, generate, and report to OH on the required Hands-On-Keyboard end-user information.	1) As part of solution testing and prior to allowing solution into production. 2) Privacy recommends a period of 1 to 2 years post-implementation period for this time-limited exception period	Short Term: 1) Affected HICs will be required to produce a Privacy Audit Report to OH as specified by privacy recommendations and applicable agreements, and in a timely manner. This report will be verified to ensure the transaction data can be traced back to the HIC organization as per PHIPA requirements. Long Term 2) Applicable HICs and their HIS solution vendors will be required to make changes such that 'Hands-on-Keyboard' information is provided to OH in the message transaction, in adherence to OH message specifications	1) Closed 2) In-Progress (see Residual Risk below)
PIA-0093	HIS-OLIS Direct Integration PIA	OLIS; potentially all EHR repositories	2022-06-02	Residual Risk #1 – There is a risk that HIS solution Vendor(s) will not make changes to the solution on a timely basis after being allowed temporary exception and/or ability to report via Privacy Audit Report Method to address Recommendation PIA-0093-01.	**PIA-0093-02:** OH Business should develop a strategic plan that addresses and mitigates this risk in a manner that ensures HIS changes are made provincially and not just for a specific, immediate HIC or HIS integration.	3 months from go-live to develop mitigation plan.	OH Business will develop a strategic plan to mitigate this risk in accordance with the recommendation. For the transactional message changes, Privacy recommends an exception period of 1 to 2 years to accomplish such changes.	In Progress

PIA ID	Name of the Reviewed Existing or Proposed System & Type of Assessment	Type(s) of PHI retrieved, processed, or integrated	Date PIA completed (YYYY-MM-DD)	Summary of Residual Risk Description	Recommendation ID & Summary of Recommendations	Date recommendation was addressed or expected to be addressed. (YYYY-MM-DD)	The manner each recommendation was or is expected to be addressed	Status
PIA-0099	PCR MDM 11.6 Upgrade R2 OCP4.8 Migration PTA	PCR	2022-06-21	No risks identified.	There were no recommendations made.	N/A	N/A	Closed
PIA-0104	One Access Gateway Upgrade and Migration to ECP - R3 PTA	All EHR repositories	2022-07-07	No risks identified.	There were no recommendations made.	N/A	N/A	Closed

Appendix C – Privacy Audits

Type and Nature of Audit	Date of Audit	Date Audit was Completed	Recommendation Made	The date each recommendation was addressed or is proposed to be addressed; and the manner in which each recommendation was addressed or is proposed to be addressed.
Privacy Audit of Procurements Audit of procurements at OH to verify that procurements involving PI/PHI were correctly identified and recorded, and then privacy review occurred. The purpose of the audit was to assess compliance to privacy policy, procedures, and practices.	Monthly from March 2021 to present	N/A - Ongoing monthly audit to review list of all new procurements.	No Recommendations were made	No Recommendations were made
Privacy Audit of Access Permissions to PHI Access certification campaigns are conducted by the Security Identity and Access Management (IAM) team annually. This includes an attestation requirement to confirm that privileged access to PHI is still required/permitted.	July 2021	September 2021 .	Revoke the privileged access for those individuals who were identified as no longer requiring access.	Access was revoked September 2021
Privacy Audit of Access Permissions to PHI A continuous certificate campaign is conducted for all individuals who have changed roles or department within OH. This involves the review of their privileged access permission to PHI to ensure that this access is still required. This review occurs throughout the year when the individual changes roles or departments.	Continuous	Continuous	Revoke the privileged access for those individuals who were identified as no longer requiring access.	Continuous
Audit of Privacy and Security Training Review of Privacy and Security Training completion logs to verify agents enrolled in courses have completed training.	Q1 2022/23	Privacy Office	During the review, it was identified that not all OH agents who were enrolled in privacy and security training in 2021 and 2020 had completed the training. It is recommended that Human Resources review and update training processes to ensure all OH agents enrolled in the privacy and security training courses for 2022 complete the required training.	Training process has been reviewed to ensure all OH agents complete the 2022 Privacy and Security Training courses. The 2022 Privacy and Security training campaign is currently in progress and is expected to be completed on September 1, 2022.

Type and Nature of Audit	Date of Audit	Date Audit was Completed	Recommendation Made	The date each recommendation was addressed or is proposed to be addressed; and the manner in which each recommendation was addressed or is proposed to be addressed.
Audit of Confidentiality Agreements Review of completed confidentiality agreement records to verify new OH agents have acknowledged and agreed to the terms of the OH Confidentiality Agreement.	Q1 2022/23	Privacy Office	During the review, it was identified that due to changes in the onboarding process from legacy eHO to OH, not all individuals being hired by OH were signing the required OH Confidentiality Agreement. It is recommended that Human Resources deploy the OH confidentiality agreement to all OH agents for 2022, and review and update the onboarding process to ensure new hires complete the OH Confidentiality Agreement.	The onboarding process has been revised to ensure that all new hires sign the OH Confidentiality Agreement. Additionally, the OH Confidentiality Agreement has been deployed to all OH Agents as part of the privacy and training campaign, that is targeted to be complete by September 1, 2022.

Appendix D – Privacy Breaches

ID	Caused By - OH - EHR system unauthorized party (not a HIC or OH)	Suspected or Actual & Breach of Policy or PHI	Nature and Scope of Breach	Cause of Privacy Breach	Date OH Sr. Management Notified	Containment Measures & Date Implemented	Date that notification was provided to HIC or other Org.	Date Investigation was commenced and completed	Recommendations made and date it is or will be addressed	Manner in which recommendation was or will be addressed
1	OH	Privacy Breach	An OH team member requested a consent directive form from the privacy team to send to an external requestor (HINP) who was requesting the form on behalf of a hospital (HIC). The form that was provided to the OH team member by a privacy team member was a completed form, rather than a blank template. The form was sent to the HINP by email and the HINP forwarded the form to the HIC. The information on the form included requestor/individual's name, HCN, address, phone number, and consent directive request details.	Human Error. A completed consent directive form was pulled from the OH staff members downloads, rather than a blank template.	February 9, 2022	The HIC identified the breach and notified the HINP, who then notified OH. All parties were instructed to securely and permanently delete the form that was communicated through email. All parties confirmed this containment measure was completed. Containment measures were implemented: January 24 to January 25, 2022	January 24 to January 25, 2022	Commenced: January 24, 2022 Completed: February 10, 2022	All team members (where the breach originated) to ensure the auto-download feature in their browser settings was set to "off". All team members to regularly review and delete items containing PI/PHI from their Downloads. The recommendations were addressed: February 2022	The recommendations were addressed via team meeting and follow up confirmation with team members to confirm the recommendations were implemented.
2	OH	Privacy Breach	An OH privacy team member sent two Consent Override Notices to the wrong HIC with the same name. First name, last name, and middle initial were the same. PHI included HCN, patient name, date of consent override, and physician who performed the override.	Multiple HIC's with the same name.	N/A - severity level for this breach was Low, not requiring Senior Management Notification. Manager was notified.	HIC who received the notification in error was instructed to securely and permanently delete the notification that was sent through email. HIC confirmed this containment measure was completed. Containment measures were implemented: March 21, 2022, to March 22, 2022	March 21, 2022	Commenced: March 21, 2022 Completed: March 22, 2022	Privacy team members to continue to validate multiple identifiers where applicable before sending PHI to HIC. The recommendations were addressed: March 2022 and ongoing	Ongoing in the day-to-day processes of the privacy team.

ID	Caused By - OH - EHR system - unauthorized party (not a HIC or OH)	Suspected or Actual & Breach of Policy or PHI	Nature and Scope of Breach	Cause of Privacy Breach	Date OH Sr. Management Notified	Containment Measures & Date Implemented	Date that notification was provided to HIC or other Org.	Date Investigation was commenced and completed	Recommendations made and date it is or will be addressed	Manner in which recommendation was or will be addressed
3	OH	Privacy Breach	An OH privacy team member sent two Consent Override Notices to the wrong HIC with a similar name. PHI included HCN, patient name, date of consent override, and HIC and agent that performed the override.	TBD	N/A - severity level for this breach was Low, not requiring Senior Management Notification.	HIC contact who received the notifications in error was instructed to securely and permanently delete the notifications sent through email. Contact confirmed this containment measure was completed. Containment measures were implemented: July 19, 2022	July 19, 2022	Commenced: July 5, 2022 Completed: ongoing	TBD – investigation in progress	TBD
4	OH	Privacy Breach	An OH privacy team member sent a Consent Override Notice to the wrong HIC with the same name (First and Last name same). PHI included HCN, patient name, date of consent override, and the physician who performed the override.	Multiple HIC's with the same name.	N/A - severity level for this breach was Low, not requiring Senior Management Notification.	HIC who received the notification in error was instructed to securely and permanently delete the notification that was sent through email. HIC confirmed this containment measure was completed. Containment measures were implemented: August 2, 2022 to August 15, 2022	August 2, 2022	Commenced: August 2, 2022	Privacy team members to continue to validate multiple identifiers where applicable before sending PHI to HIC. Continue to work with the onboarding team to confirm HIC's and contacts.	Ongoing in the day-to-day processes of the privacy team.

Appendix E – Privacy Complaints

Activity #	Date privacy complaint received	Nature of the privacy complaint	Date the investigation commenced	Date of the written communication to the individual who made the privacy complaint	Date that the investigation was completed	Results of Investigation & Description of each recommendation made	Date each recommendation was addressed, or is proposed to be addressed	Manner in which each recommendation was addressed, or is proposed to be addressed	Date of the written communication to the individual made the privacy complaint in relation to the commencement investigation and the measures taken in response to the complaint
N/A									

Appendix F – General Security Policies and Procedures

Name of Policy or Document	Date the policy was reviewed for OH approval or PO submission	Amendments (Y/N) or New	Description of Amendment or new policy or document	Date and nature of policy communications to employees and other persons acting on behalf of OH	Whether communication materials available to public
Access Card Procedure	29-Apr-21	New	New Procedure based on the legacy Cancer Care Ontario Procedure. This Procedure provides the process steps for the issuance, use, revocation, and accountability of Access Cards that control access to OH Offices.	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on the Pulse on the harmonization of legacy policies and developing new enterprise policies.	N/A
Access Control Standard	29-Apr-21	New	New Standard based on the legacy eHealth Ontario Standard with the same name and the Identity and Password Standard. This Standard establishes security requirements regarding logical access to Ontario Health Assets. Updated requirements for domain on-premises and cloud-based authentication for regular OH user accounts, for user ID and password management, definitions, and requirements from the IPC's Manual for the Review and Approval of Prescribed Organizations for Access to Personal Health Information (PHI).	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on the Pulse on the harmonization of legacy policies and developing new enterprise policies.	N/A
Cryptography Standard	29-Apr-21	Y	First approved and published on 25-Sept-20. Based on the legacy eHealth Ontario and Cancer Care Ontario Standard with the same name. Updated FIPS to 140-3, the list of Approved Cryptographic Algorithms, and the definitions.	March 15, 2022: Published on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A
External Information Security Incident Management Standard	29-Apr-21	New	New Standard based on the legacy eHealth Ontario Standard. The Standard outlines Information Security Incident Management practices, roles and responsibilities between Ontario Health and external stakeholders of Ontario Health, such as Health Information Custodians, Agents and Electronic Service Providers or any third party retained by Ontario Health. Minor changes made to meet the requirements from the IPC's Manual for the Review and Approval of Prescribed Organizations, to align with new definitions and terms, and adopt the new OH template.	The communications materials to be amended as a result of the review will be determined as part of a communications plan, the timelines for which will be communicated to the IPC.	N/A
	15-Sep-21	Y	Updated to incorporate IPC PO Manual Requirements Updated to reflect updated OH roles and responsibilities, and accountabilities structures Updated scope and policies to include all OH legacy organizations	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on the Pulse on the harmonization of legacy policies and developing new enterprise policies.	N/A

Name of Policy or Document	Date the policy was reviewed for OH approval or PO submission	Amendments (Y/N) or New	Description of Amendment or new policy or document	Date and nature of policy communications to employees and other persons acting on behalf of OH	Whether communication materials available to public ...
Hard Copy PHI/PI and Media Destruction Procedure	29-Apr-21	New	New Procedure based on the legacy Cancer Care Ontario Procedure. The Procedure supports the Media Destruction, Sanitization and Disposal Standard by further providing the process steps for implementing the secure destruction of hard-copy records containing personal health information (PHI) and/or personal information (PI), which must be disposed of in a secure manner. In addition, this Procedure documents the supporting role of Facilities in secure media destruction.	The communications materials to be amended as a result of the review will be determined as part of a communications plan, the timelines for which will be communicated to the IPC.	N/A
	15-Sep-21	Y	Reflects updated OH roles and responsibilities and accountabilities structures. Scope and policies include all OH legacy organizations.	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on the Pulse on the harmonization of legacy policies and developing new enterprise policies.	N/A
Information Classification and Handling Guideline	29-Apr-21	Y	The Information Classification and Handling Guideline was first approved and published on 15-Jul-20. It is based on the legacy Cancer Care Ontario Guideline with the same name. Updates were made to meet the requirements from the IPC's Manual for the Review and Approval of Prescribed Organizations.	V1.0 was published on 15-Jul-20 on the OH corporate intranet. Published Security Policies were communicated via Mandatory Training for Privacy and Security rolled out on 25-May-21 -- see Appendix I. Updated version – The communications materials to be amended as a result of the review will be determined as part of a communications plan, the timelines for which will be communicated to the IPC.	N/A
	15-Sep-21	Y	Updates to reflect updated OH roles and responsibilities, and accountabilities structures Scope and policies to include all OH legacy organizations	March 30, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A
Information Classification and Handling Standard	29-Apr-21	Y	The Information Classification and Handling Standard was first approved and published on 15-Jul-20. It is based on the legacy Cancer Care Ontario Standard with the same name. This Standard is supported by the Information Classification and Handling Guideline. Updates were made to meet the requirements from the IPC's Manual for the Review and Approval of Prescribed Organizations.	Published Security Policies were communicated via Mandatory Training for Privacy and Security rolled out on 25-May-21 -- see Appendix I. March 30, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A

Name of Policy or Document	Date the policy was reviewed for OH approval or PO submission	Amendments (Y/N) or New	Description of Amendment or new policy or document	Date and nature of policy communications to employees and other persons acting on behalf of OH	Whether communication materials available to public ...
Information Security Acceptable Use Policy	28-Oct-20	New	The Information Security Acceptable Use Policy was first approved and published on 28-Oct-20. It is based on legacy policies from eHealth Ontario and Cancer Care Ontario. The Policy defines OH's commitment to ensure the safeguarding of OH Information Assets by establishing clear behavioral expectations for those authorized persons who use OH resources	V1.0 was published on 28-Oct-20 on the OH corporate intranet. Published Security Policies were communicated via Mandatory Training for Privacy and Security rolled out on 25-May-21 – see Appendix I.	N/A
	11-Nov-21	Y	Updates to reflect updated OH roles and responsibilities, and accountabilities structures. Scope and policies include all OH legacy organizations.	April 20, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A
Information Security Incident Management Standard	13-Oct-20	New	The Information Security Incident Management Standard was first approved and published on 13-Oct-20. It is based on legacy policies from eHealth Ontario and Cancer Care Ontario. The Standard establishes a consistent and effective approach to the management of Cyber Security Incidents, including communication on Cyber Security Events and Vulnerabilities.	V1.0 was published on 13-Oct-20 on the OH corporate intranet. Published Security Policies were communicated via Mandatory Training for Privacy and Security rolled out on 25-May-21 – see Appendix I.	N/A
	15-Sep-21	Y	Updates were made to distinguish internal communications from external communications covered in the External Information Security Incident Management Standard. Updated the responsibilities of teams/functions responsible for incident response and resolution. Updated to align with requirements from the IPC's Manual for the Review and Approval of Prescribed Organizations. Updated to new definitions, terminology, and the new OH template.	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A

Name of Policy or Document	Date the policy was reviewed for OH approval or PO submission	Amendments (Y/N) or New	Description of Amendment or new policy or document	Date and nature of policy communications to employees and other persons acting on behalf of OH	Whether communication materials available to public
Information Security Operations Standard	29-Apr-21	Y	The Information Security Operations Standard was first approved and published on 15-Jul-20. It is based on the legacy eHealth Ontario Standard. The Standard outlines the security requirements necessary to operate information processing environments in OH. In section 2.2 "Change Management", updates were made to reflect approval/rejection of changes to the operational environment, testing and documentation. In section 2.6 "Backup", amendments were made to reflect general processes and processes involving PHI and retention of PHI records. Updated controls within section 2.7 "Logging and Monitoring". Updated 2.11.1 "General Requirements" for patch management, patch analysis and required documentation. Updates were made to meet the requirements from the IPC's Manual for the Review and Approval of Prescribed Organizations.	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A
Information Security Policy	23-Sep-21	New	New Policy based on the legacy eHealth Ontario and Cancer Care Ontario Policies. This Policy defines OH's commitment to information security and sets out the requirements for information security practices within OH. Updates were made to meet the requirements from the IPC's Manual for the Review and Approval of Prescribed Organizations and reflect updated OH roles and responsibilities, and accountabilities structures. Scope and policies include all OH legacy organizations. Supersedes the **Error! Reference source not found.** and the **Error! Reference source not found.**	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A
Information Security Program Governance	29-Apr-21	New	New Policy that complements the Information Security Policy. It provides a description of how oversight of and accountability for OH's security program is organized within OH. Updates were made to meet the requirements from the IPC's Manual for the Review and Approval of Prescribed Organizations.	The communications materials to be amended as a result of the review will be determined as part of a communications plan, the timelines for which will be communicated to the IPC.	N/A
	11-Nov-21	Y	Updates to reflect updated OH roles and responsibilities, and accountabilities structures. Scope and policies include all OH legacy organizations.	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A

Name of Policy or Document	Date the policy was reviewed for OH approval or PO submission	Amendments (Y/N) or New	Description of Amendment or new policy or document	Date and nature of policy communications to employees and other persons acting on behalf of OH	Whether communication materials available to public
Information Security Risk Management Standard	15-Sep-21	New	New Standard based on the legacy Cancer Care Ontario and eHealth Ontario Standards: Information Security Risk Management Standard and Information Security Compliance Standard. The Standard identifies the circumstances in which and approaches by which OH conducts security audits and identifies, assesses, responds to, and monitors information security risks. Updates were made to meet the requirements from the IPC's Manual for the Review and Approval of Prescribed Organizations.	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A
Information Security Software & Systems Standard	29-Apr-21	Y	The Information Security Software & Systems Standard was first approved and published on 15-Jul-20. It is based on the legacy eHealth Ontario Standard. The Standard outlines the context and requirements for the design of applications with secure software standards at OH. Updated controls within section 2.8.10 "User Acceptance Testing". Updates were made to meet the requirements from the IPC's Manual for the Review and Approval of Prescribed Organizations.	Published Security Policies were communicated via Mandatory Training for Privacy and Security rolled out on 25-May-21 – see Appendix I. March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A
Media Destruction, Sanitization, and Disposal Standard	29-Apr-21	New	New Standard based on the legacy Cancer Care Ontario and eHealth Ontario Standards. It specifies the mandatory requirements and roles and responsibilities to ensure secure decommissioning, destruction, sanitization, and disposal of Media appropriate for the sensitivity of information stored within. Updates were made to meet the requirements from the IPC's Manual for the Review and Approval of Prescribed Organizations.	The communications materials to be amended as a result of the review will be determined as part of a communications plan, the timelines for which will be communicated to the IPC.	N/A
	15-Sep-21	Y	Updates to address PE/PP Manual requirements. Scope and policies include all OH legacy organizations. Supersedes the **Error! Reference source not found.** and the **Error! Reference source not found.**	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A
Mobile Security Standard	29-Apr-21	New	New Standard (originally titled the Mobile Computing Security Standard) based on the legacy eHealth Ontario Standard. It describes security requirements for the use of mobile devices at OH. Added in section 2.11 "Non-OH Managed Mobile Communication Device". Updates were made to meet the requirements from the IPC's Manual for the Review and Approval of Prescribed Organizations.	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A

Name of Policy or Document	Date the policy was reviewed for OH approval or PO submission	Amendments (Y/N) or New	Description of Amendment or new policy or document	Date and nature of policy communications to employees and other persons acting on behalf of OH	Whether communication materials available to public
Network Security and Communications Standard	29-Apr-21	New	New Standard based on the legacy eHealth Ontario Standard with the same name. Update hardening of the demilitarized zone (DMZ). Updates were made to meet the requirements from the IPC's Manual for the Review and Approval of Prescribed Organizations.	The communications materials to be amended as a result of the review will be determined as part of a communications plan, the timelines for which will be communicated to the IPC.	N/A
	15-Sep-21	Y	Reflects OH roles and responsibilities, and accountabilities structures. Scope and policies include all OH legacy organizations.	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A
Personal Health Information Handling Standard	29-Apr-21	New	New Standard based on the legacy Cancer Care Ontario Standard with the same name. The purpose of this Standard is to establish a framework of approved methods and safeguards for ensuring the secure handling of personal health information (PHI) so that OH continues to meet its obligations under Ontario's Personal Health Information Protection Act, 2004 (PHIPA).	The communications materials to be amended as a result of the review will be determined as part of a communications plan, the timelines for which will be communicated to the IPC.	N/A
	15-Sep-21	Y	Updated to reflect updated OH roles and responsibilities, and accountabilities structures. Scope and policies include all OH legacy organizations.	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A
Physical Access Policy	29-Apr-21	New	New Policy based on the legacy Cancer Care Ontario Policy. The Policy describes the high-level organizational requirements for physical access to the physical environments operated by OH.	The communications materials to be amended as a result of the review will be determined as part of a communications plan, the timelines for which will be communicated to the IPC.	N/A
	15-Sep-21	Y	Updated to incorporate IPC PO Manual Requirements and reflects OH roles and responsibilities, and accountabilities structures. Scope and policies include all OH legacy organizations.	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A

Name of Policy or Document	Date the policy was reviewed for OH approval or PO submission	Amendments (Y/N) or New	Description of Amendment or new policy or document	Date and nature of policy communications to employees and other persons acting on behalf of OH	Whether communication materials available to public
Physical and Environmental Security Standard	28-Oct-20	New	Based on the legacy Cancer Care Ontario Policy, the policy describes the high-level organizational requirements for physical access to the physical environments operated by OH. The Physical and Environmental Security Standard was first approved and published on 28-Oct-20. It establishes requirements, management and technical controls to safeguard PHI and information technology resources from unauthorized physical access	V1.0 was published on 28-Oct-20 on the OH corporate intranet. Published Security Policies were communicated via Mandatory Training for Privacy and Security rolled out on 25-May-21 – see Appendix I.	N/A
	29-Apr-21	Y	Updates were made to meet the requirements from the IPC's Manual for the Review and Approval of Prescribed Organizations. Updated responsibilities of various departments with regards to Physical Security. Updated definitions and terminology and adopted the new OH template.	The communications materials to be amended as a result of the review will be determined as part of a communications plan, the timelines for which will be communicated to the IPC.	N/A
	15-Sep-21	Y	Updated to reflect OH roles and responsibilities, and accountabilities structures. Scope and policies include all OH legacy organizations.	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A
Secure Transfer of Sensitive Information Standard	29-Apr-21	New	New Standard based on legacy Cancer Care Ontario Standards and Procedures. The Standard ensures the protection of Personal Information (PI) and PHI in accordance with PHIPA and FIPPA when said information is transferred, processed, and received. Updates were made to meet the requirements from the IPC's Manual for the Review and Approval of Prescribed Organizations.	The communications materials to be amended as a result of the review will be determined as part of a communications plan, the timelines for which will be communicated to the IPC.	N/A
	15-Sep-21	Y	Updates were made to reflect updated OH roles and responsibilities, and accountabilities structures. Scope and policies include all OH legacy organizations.	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A
Video Monitoring Policy	29-Apr-21	New	New Policy based on the legacy Cancer Care Ontario Policy. The Policy establishes the requirements for the installation, maintenance and use of video monitoring technologies on OH Premises.	The communications materials to be amended as a result of the review will be determined as part of a communications plan, the timelines for which will be communicated to the IPC.	N/A

Name of Policy or Document	Date the policy was reviewed for OH approval or PO submission	Amendments (Y/N) or New	Description of Amendment or new policy or document	Date and nature of policy communications to employees and other persons acting on behalf of OH	Whether communication materials available to public ...
Video Monitoring Procedure	29-Apr-21	New	New Procedure based on the legacy Cancer Care Ontario Procedure. The document outlines the procedures for video monitoring at OH Premises.	The communications materials to be amended as a result of the review will be determined as part of a communications plan, the timelines for which will be communicated to the IPC.	N/A
	15-Sep-21	Y	Updated to reflect OH roles and responsibilities, and accountabilities structures. Scope and policies include all OH legacy organizations.	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A
Visitor Access Procedure	29-Apr-21	New	New Procedure based on the legacy Cancer Care Ontario Procedure. The Procedure outlines the steps that must be followed by OH Agents when hosting Visitors at OH Offices.	The communications materials to be amended as a result of the review will be determined as part of a communications plan, the timelines for which will be communicated to the IPC.	N/A
	15-Sep-21	Y	Updated to reflect updated OH roles and responsibilities and accountabilities structures. Scope and policies include all OH legacy organizations.	March 15, 2022: Published the new standards on the OH Policy Hub (Intranet). May 17, 2022: Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	N/A

Appendix G – Security Audits

Security Audit	Description	Date of Audit	Recommendation	Expected Remediation Date	Remediation Plan
Laboratory Information Management System (LIMS)	Potential vulnerabilities in the new interface code	2021-09-09	External data partner is planning a software update that will begin in early 2022. A new TRA, Vulnerability Scan and Penetration Test will be carried out as part of that project.	Mid 2022	External data partner is planning a software update that will begin in early 2022. A new TRA, Vulnerability Scan and Penetration Test will be carried out as part of that project.
OLIS Hub Management Console	Vulnerabilities In OLIS Hub Management Console	2021-11-08	Upgrade of the ONE ID Oracle OAM platform to version 12c will allow the Oracle Java JRE to be updated to a supported version.	2022-04-27	Upgrade of the ONE ID Oracle OAM platform to version 12c will allow the Oracle Java JRE to be updated to a supported version.
Kafka Infrastructure	Missing Security patches on Linux Red Hat Servers for Kafka Infrastructure	2021-11-08	1. Migration from v 3.1.X of Kafka IBM Event Streams Platform to v 3.2.X Kafka IBM Event Stream Platform, which supports RHEL v 7.7 and later. 2. Once IBM Events Streams container platform is supported on OpenShift, we will deploy the IBM Events Streams on our enterprise container platform (OpenShift version 4.4). The OS version for OpenShift will be at least RHEL 7.8 or later.	2022-10-20	1. Migration from v 3.1.X of Kafka IBM Event Streams Platform to v 3.2.X Kafka IBM Event Stream Platform, which supports RHEL v 7.7 and later. 2. Once IBM Events Streams container platform is supported on OpenShift, we will deploy the IBM Events Streams on our enterprise container platform (OpenShift version 4.4). The OS version for OpenShift will be at least RHEL 7.8 or later.
Threat and Risk Assessment	Installed Applications and Configuration of the new laptop for Employees.	2022-03-31	Recommendations to fix mitigate the risks	Prior to deployment	Risks will be address prior to configuration/deployment of OH hardware.
Penetration Test	External and Internal Network Penetration test of new laptop configuration.	2022-05-06	Recommendations to fix the identified Vulnerabilities	In progress	Address vulnerabilities prior to configuration/deployment of OH hardware.
3rd Party Security Assessment	Ontario Health Cyber Security Maturity Assessment of Enterprise Services Internal Controls	November 2021 – ongoing	TBD	TBD	TBD
Security Assessment	Connecting Ontario 10.8	6/30/2022	Address vulnerabilities from Vulnerability Assessment scan.	TBD	TBD

Appendix H – Security Breaches and Suspected Security Breaches

Security breaches or suspected security breaches caused by the prescribed organization; a system that retrieves, processes or integrates personal health information in the electronic health record; or a person who is not an employee or other person acting on behalf of the prescribed organization or an agent or electronic service provider of a health information custodian since the prior review by the IPC:

Incident #	Incident date	Breach of EHR PHI	Caused by: 1) A person who is not an Agent of OH, or an Agent or Electronic Service Provider (ESP) of a HIC; 2) OH; or 3) OH system that retrieves, processes, or integrates PHI?	Nature and scope of breach or suspected breach	Cause of breach or suspected breach	Date senior management was notified	Containment measures and Date of Containment Measures	Date notification was provided to HIC or other orgs	Date investigation was commenced	Date investigation was completed	Description of each recommendation made	Date recommendation addressed/will be addressed	Status of recommendation
INC000000391559 3	3-Dec-21	No	2) OH	Possible OH compromised account reported by HIC. Email originating from an OH mailbox contained executables and instructions for installing and running within a timeframe and imparting a sense of urgency. Policy violation (AUP)	OH employee sent emails to HICs instructing recipients to install the attached applications / tools then execute them. OH employee did not review or discuss their requirements with IT at OH or the HIC.	3-Dec-21	3-Dec-21: HIC blocked all further communications from the OH employee's @ontariohealth.ca mailbox. Communicated the cybersecurity incident to MGCS. Communicated the cybersecurity incident to OH. The cybersecurity incident was reported to OH CSIRT for further analyses.	N/A	3-Dec-21	3-Dec-21	CSIRT / HIC meeting. Determined the OH employee intended the action; however, they were not authorized to install applications and other tools and execute them on hospital systems without engaging IT. Engaged privacy to discuss steps and processes to deploy software on Hospital infrastructure.	4-Dec-21	Complete

Appendix I – Privacy and Security Communications

Privacy Communications Log

Training/Awareness Activity	Communication Type	Date of Communication
Privacy role-based training for the Privacy Staff: PHIPA roles and authorities	Virtual/Online	June 2, 2021
Privacy and Security presentation/review of the OH 2020/21 Annual Privacy and Security Report to Senior Leadership Team	Email/Meeting Materials	June 9, 2021
Privacy role-based training for the Privacy Staff: Role of the IPC	Virtual/Online	June 16, 2021
Privacy role-based training for the Privacy Staff: De-identification	Virtual/Online	Part 1; June 2021 Part 2: October, 2021
Privacy and Security presentation/review of the OH 2020/21 Annual Privacy and Security Report to the OH Board	Virtual/Online	June 23, 2021
Privacy role-based training for the Privacy Staff: Data Sharing Agreements	Virtual/Online	September, 2021
Privacy role-based training for the Privacy Staff: Prescribed Organization and EHR	Virtual/Online	November, 2021
Privacy authorities overview – Datasphere WG	Virtual/Online	December 2021
Privacy role-based training for the Privacy Staff: Information Security	Virtual/Online	January 26th, 2022
Message to all staff posted to the OH intranet page for Annual Privacy Day emphasizing the importance of privacy, OH's commitment and role in protecting privacy in accordance with PHIPA	Intranet	January 28, 2022
Portfolio Fair – Privacy Presentation for available to all OH staff	Virtual/Online	March, 2022
Privacy role-based training for the Privacy Staff: Privacy Incident Management	Virtual/Online	March 9th 2022
Privacy role-based training for the Privacy Staff: Data Architecture	Virtual/Online	April, 2022
Privacy role-based training for the Privacy Staff: PIAs remember the objective	Virtual/Online	May 4, 2022
All staff email re: Published the new standards on the OH Policy Hub	All staff email	May 2022
Article published on *the Pulse* on the harmonization of legacy policies and developing new enterprise policies.	Intranet	May 17, 2022
Mandatory Training for Privacy and Security email to all staff notifying them of the upcoming enrollment of mandatory privacy and security training, and OH's compliance requirements for all employees and agents to complete the training.	Email	June, 2022
Annual Privacy & Security Report – 2021/22 presented to the ITC Board Committee	Virtual/Online	June 21, 2022
Privacy and Security presentation/review of the OH 2012/22 Annual Privacy and Security Report to Senior Leadership Team	Email/Meeting Materials	June, 2022

Security Communications Log

Training/Awareness Activity	Communication Type	Date of Communication
Cyber Security Update	Materials presented to Information Technology Committee (ITC)	5/25/2021
Phishing Simulations	The Pulse (OH Intranet) Post	6/11/2021
Monthly Phishing Simulation Campaign – June 2021	Email	6/16/2021
1) Annual Privacy & Security Report – 2020/21; and, 2) Updates from Cyber Security Education Session: Security Breach Escalation Path	Materials presented to ITC	6/22/2021
Monthly Phishing Simulation Campaign – August 2021	Email	8/16/2021
Did you know you can report phishing from your Outlook?	The Pulse (OH Intranet) Post	8/10/2021
Ontario Health Phishing Simulation	Email	9/1/2021
Monthly Phishing Simulation Campaign – September 2021	Email	9/13/2021
Join us for Cyber Security Awareness Month	The Pulse (OH Intranet) Post	10/22/2021
Monthly Phishing Simulation Campaign – October 2021	Email	10/27/2021
Monthly Phishing Simulation Campaign – November 2021	Email	11/1/2021
Security Training for Finance and Procurement	Email	11/16/2021
Cyber Security Report	Materials presented to ITC	11/23/2021
Digital Health Week – Ontario Health Highlights	The Pulse (OH Intranet) Post	12/3/2021
Monthly Phishing Simulation Campaign – December 2021	Email	12/14/2021
Monthly Phishing Simulation Campaign – January 2022	Email	1/21/2022
Monthly Phishing Simulation Campaign – Feb 2022	Email	2/25/2022
Monthly Phishing Simulation Campaign – Mar 2022	Email	3/22/2022
Cyber Security Report	Materials presented to ITC	3/23/2022
Monthly Phishing Simulation Campaign – Apr 2022	Email	4/22/2022
Monthly Phishing Simulation Campaign – May 2022	Email	5/27/2022
Annual Privacy & Security Report – 2021/22	Materials presented to ITC	6/21/2022
Daily Threat Intelligence Brief	External service providers, legacy Shared Services staff, Provincial-Privacy Officers, OH Cyber Security Defense	Daily
2022 Privacy and Security Training	All Staff	6/12/2022
Monthly Phishing Simulation Campaign – June 2022	Email	6/29/2022
Monthly Phishing Simulation Campaign – July 2022	Email	7/25/2022

Appendix J – Business Continuity & Disaster Recovery Table-top Testing Log

Department Name	Tabletop Test Date	Comments / Amendments to Plan
Cyber Security Defense	April 5-2022	Update Business function 4.0) change MTO to 3+ days. Update staff requirements table, add link for document location
Platform & Cloud Operations	April 7-2022	Service provider information to be updated
IT Service Management	April 7-2022	Apps, recovery info, external clients, contact information, staffing requirements, document location information to be updated
Tech Planning Continuity	April 12-2022	Follow up meeting with IT Service Management on the incident management process, engage HR on the Incident management hotline (updating etc.)
Product Mgmt & Customer Value	April 22-2022	Business functions to be updated
Cyber Security Governance	April 13-2022	Business functions, and contact information to be updated
Product Management Delivery	April 13-2022	Staffing requirements and contact information to be updated
Product Mgmt & Cust Value	March 29-2022	Business function MTO and document URL location to be updated
Project Governance	March 10-2022	N/A
Product Mgmt & Cust Value & Products	March 7-2022	N/A
Product Mgmt & Cust Value & Products	March 24-2022	Contact information to be updated
Data Centre Services	March 9-2022	N/A
Digital Health Standards	March 15-2022	Contact information to be updated
Digital Strategy Management	March 17-2022	Contact and business function procedures location information to be updated
Product Mgmt & Customer Value	March 24-2022	N/A
Product Mgmt & Cust Value & Products	March 8-2022	Contact information to be updated
Customer Experience	March 8-2022	N/A
Customer Experience & Business	March 4-2022	N/A
Cloud Centre of Excellence	March 15-2022	N/A
Architecture Program	March 17-2022	N/A
Network Services	March 22-2022	N/A
Transformation Centre of Excellence	March 16-2022	Contact information to be updated
Connected Health Programs	March 25-2022	Contact, required application, and procedures location information to be updated
Enterprise Products	March 18-2022	N/A
Customer Transition	March 16-2022	Service provider information to be updated