eHealth Centre of Excellence
Privacy Impact and Threat Risk Assessment Policy

v.4 March 3, 2020

Document Control

The electronic version of this document is recognized as the only valid version.

Document Location:	System Coordinated Access Program Office
Document Contributors:	Lori Moran, SCA Program Director Bosco Chan, Security Lead, SCA Program Danielle Olivier-Ozutok, PM, SCA Program
Document Prime:*	Sylvia Carney, Senior Privacy Analyst

*Enquiries relating to this document should be referred to the Document Prime.

Revision History

Version No.	Date	Summary of Change	Revised By
[1]	Sept 20, 2017	Initial Draft	J Montgomery
[2]	Jan 17, 2018	Review by Think Research Privacy WG – terminology updated	J Vaianisi
[3]	Jan 17, 2018	Revisions Accepted – terminology updates accepted	J Montgomery
[4]	March 3, 2020	Name change, more broadly applicable; various other content changes	S. Carney
[5]			

Approval History

Approver	Title	Approved Date
Leslie Macumber	Program Director	March 16, 2020

Purpose of Policy

With a vision to develop best practices and enable technology to support improved clinical care, the eHealth Centre of Excellence (eCE) promotes privacy and information security at all stages of the information lifecycle. Effective, coordinated and secure system access requires integration of various tools and technologies. The eCE is committed as a digital health enabler and Health Information Network Provider, to protect the privacy and confidentiality of Personal Information (PI) including Personal Health Information (PHI) that is collected, used, disclosed or retained as part of the eCE electronic healthcare technology network.

The eCE Privacy Impact Assessment (PIA) and Threat Risk Assessment (TRA) Policy establishes the requirements of an organizational PIA and TRA framework. Solution Providers/vendors desiring to integrate with or provide electronic services to the eCE are obligated to adhere to this policy. PIA/TRA requirements are communicated in early negotiations and committed to via a contractual agreement.

The eCE will ensure fair and consistent evaluation by requiring the use of industry standard templates which conform to the Information Privacy Commissioner (Ontario) guidelines, Privacy by Design methodology, Harmonized TRA, NIST and/or ISO/ISF framework. See Reference Documents.

When an independent third party is contracted to complete the PIA/TRA assessments, the eCE is responsible to ensure that the third party has no conflict of interest and follows, at a minimum, the foundational principles outlined in this policy.

This policy addresses the particular requirements of a HINP to perform, and provide to each applicable health information custodian a written copy of the results of, an assessment of the services provided to the health information custodians, with respect to:

- threats, vulnerabilities and risks to the security and integrity of the personal health information; and
- how the services may affect the privacy of the individuals who are the subject of the information.

The eCE has sought input from internal Privacy and Security leadership. the Information Privacy Commissioner of Ontario, Canada Health Infoway, and eHealth Ontario to inform this policy.

PIA/TRA Assessment Methodology - Foundational Principles

A Privacy Impact Assessment (PIA) and Threat Risk Assessment (TRA) are formal risk management tools that include consideration of other risk management and due diligence documents. They are used to identify actual or potential effects that a new business activity may have on an individual's privacy. A PIA and TRA will assist in identifying potential privacy and security risks associated with the new business activity, allowing accountable persons to make decisions related to acceptance, transfer or risk mitigation strategies to reduce the likelihood or impact of adverse privacy and security events.

The process of conducting a PIA and TRA provides a means for:

- analyzing privacy and security issues systematically;
- meeting legal, regulatory and/or policy requirements;

- demonstrating compliance with privacy and security obligations;
- considering potential risks; and
- developing potential solutions/mitigating strategies for the proposed business activity.

PIA/TRA assessment is a continuous process that should be maintained throughout the lifecycle of the business activity. Conducting and updating a PIA and TRA throughout the design, development, implementation and operation of a program will:

- provide valuable input into the design of the program / corresponding solution;
- help ensure that privacy and security is considered as the solution evolves; and
- ensure that the solution continues to be compliant with privacy and security obligations once deployed and operational.

The due diligence conducted during the assessment is intended to promote trust relationships between entities, ensuring appropriate collection, use, disclosure and retention of PHI in the entities' custody or control.

A PIA and TRA assessment will be conducted in the following circumstances:

- new systems interface with existing/additional systems to provide a digital solution;
- new types or roles of HIC's/HINP's or Service Providers or entities are contemplated/implemented
- there are changes to applicable agreements that might be expected to impact the privacy of individuals or the security of their PHI
- altered workflow or a material change is made to the functionality, purposes, data collection, uses, disclosures, relevant agreements or authorities for a program, initiative, process or system that are not reflected in original assessment;
- other initiatives, programs or processes are undertaken that may affect privacy and/or security;
- changes occur in the laws that govern the privacy and security of PI and PHI;
- the eCE determines that an update of a PIA or TRA or a new PIA or TRA is required

Update/refresh of an existing PIA/TRA will occur when one of the above conditions is present, or every two years at a minimum. A copy of the updated PIA/TRA will be provided to the eCE.

Privacy and Security Threshold Assessment

The eCE is responsible to ensure the completion of a Privacy and Security Threshold Assessment [Appendix A] for every new program, integration or any new initiative within an existing program. A Privacy and Security Threshold is a preliminary analysis used to determine if a service/system will require the completion of a full PIA and/or TRA.

Threshold assessments will help determine the best way the eCE can support an initiative. This could include providing advisory services, training, conducting an in-house PIA/TRA or recommending evaluation by a third party. In some cases, it may be determined that privacy/security input is not required.

Threshold Assessments will be submitted and reviewed by the respective program's Privacy, Security and Technical Leadership and Advisory Committees, and may inform a further recommendation to the eCE Executive.

Completing the Privacy Impact Assessment and/or Security Threat Risk Assessment

Contingent on available resources, a third party will generally be procured to conduct PIA/TRA on behalf of the eCE. When only a PIA is deemed necessary, the eCE Privacy Lead may complete this assessment internally using the Information Privacy Commissioner, Ontario Privacy Impact Assessment Template (See Reference Documents).

In all cases, the minimum required assessment data set will be made available for review by the respective program's Privacy, Security and Technical Leadership and Advisory Committees.
Requirements for Solution Providers

- Solution providers will engage with the eCE during the RFP, procurement or early integration phase of development.
- Solution providers who choose to provide their own PIA and/or TRAs will ensure that the assessment methodology aligns with industry standards and current best practice (IPC, Harmonized TRA, NIST, ISO/ISF)
- Solution provider will provide the results of the assessments to allow for informed evaluation/assessment. The eCE is responsible for keeping the assessment strictly confidential. Results of assessments will only be shared with authorized individuals as necessary to inform go/no go decision.
- Solution providers must remediate any high-level risks identified prior to go live of a service, all other remediation recommendations are to be implemented in time agreed upon within a risk remediation plan.
- Solution Executive PIA and/or TRA reports will be made available via the eCE Website.

Assessment Data Sets

At a minimum, the PIA Assessment will contain the following:

- Executive Summary
- Description of the solution and anticipated outcome of interface (where appropriate)
- Organizational Privacy Management & Privacy Policy Review
- Privacy Gap Analysis
- Solution Privacy Management and Technical Analysis
- List of Data Elements
- Business Process Diagram
- Data Flow Analysis and Data Flow Table
- Privacy Risk Analysis Report which identifies: risk types, threat agents, threat analysis, safeguard analysis, vulnerability analysis, current-state risk register, with risk ratings, likelihood and impact summary table
- Risk Mitigation Strategies and Recommendations

At a minimum, the TRA Assessment will contain the following:

- Executive Summary
- Summary of all Assets
- Statement of Sensitivity
- Threat Identification
- Vulnerability identification

- Security Risk Analysis Report including: risk type and threat scenario, asset sensitivity, threat analysis, safeguard analysis, vulnerability analysis, risk register
- Risk Mitigation Strategies and Recommendations

Risk Recommendations and Final Sign-off

Prior to go-live all high-level risks identified will obtain sign-off by the respective Program Director, Privacy and Security Leadership, and vendor privacy and security leads, as appropriate to the initiative, to ensure clear acceptance, transfer, or mitigation has been established and documented. Final sign off resides with eCE Executive.

Reference Documents:

https://www.ipc.on.ca/resource/planning-for-success-privacy-impact-assessment-guide/

Personal Health Information Protection Act (PHIPA, 2004)

Privacy by Design: 7 Foundational Principles

https://cyber.gc.ca/en/guidance/harmonized-tra-methodology-tra-1

https://www.nist.gov/cyberframework/framework

ISO/IEC 27002:2013 Code of Practice for Information Security Controls