PRIVACY FRAMEWORK FOR SHARED ELECTRONIC SYSTEMS

Manuela Di Re, Director of Legal Services (Acting)

Debra Grant, Director of Health Policy

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

Outline

1. Need for Governance Framework and Harmonized Privacy Policies and Procedures
2. Privacy Training and Awareness
3. Privacy Assurance
4. Logging, Auditing and Monitoring
5. Consent Management
6. Privacy Breach Management
7. Privacy Complaints and Inquiries Management
8. Access and Correction

The Need for a Governance Framework and Harmonized Privacy Policies and Procedures

Challenges Posed by Shared Electronic Systems

- Health information custodians may have custody or control of personal health information they create and contribute to, or collect from, shared electronic systems;
- However, no custodian will have sole custody and control;
- All participating health information custodians and their agents will have access to the personal health information;
- These pose privacy risks and challenges for compliance with the *Personal Health Information Protection Act* (*Act*).

Risks Posed by Shared Electronic Systems

- Shared electronic systems are only as strong in terms of privacy protection as their weakest link;
- This is a reason that a governance framework, harmonized policies and procedures and privacy training and awareness is imperative;
- Resources are often spent defending against external attacks, however, from our experience, internal threats pose an equal, if not greater, risk to privacy.

Need for Governance Framework and Harmonized Privacy Policies and Procedures

- A governance framework and harmonized privacy policies and procedures are needed to:
  - Set out the roles and responsibilities of each health information custodian participating in a shared electronic system;
  - Set out the expectations for all health information custodians and agents in accessing personal health information;
  - Ensure consistency across all health information custodians and ensure they operating under common privacy standards;
  - Set out how the rights of individuals under the *Act* will be exercised in the shared electronic system.

Governance Framework

Need to determine up front who will be responsible and the process for determining:

- Who will have access to the shared electronic system;
- What information will be included in the shared electronic system;
- The levels of access in the shared electronic system;
- The purposes for which personal health information may be collected, used and disclosed in the share electronic system;
- The nature and scope of the policies and procedures that will apply to the shared electronic system.

Nature of Harmonized Privacy Policies and Procedures

Harmonized privacy policies and procedures should be developed to address:

- Privacy training;
- Privacy assurance;
- Logging, auditing and monitoring;
- Consent management;
- Privacy breach management;
- Privacy complaints and inquiries management;
- Access and correction; and
- Governance.

Harmonized Privacy Training and Awareness Policies and Procedures

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Recommended Content Related to Privacy Training

- Person(s) responsible for the development and implementation of privacy training and awareness in the shared electronic system;
- Requirement to provide and to attend privacy training prior to accessing personal health information in the shared system;
- Requirement to provide and to attend ongoing privacy training;
- Required minimum content of privacy training materials;
- Requirement to review and refresh privacy training materials and the person(s) responsible and the frequency of this review;
- Mechanisms to foster a culture of privacy and raise awareness of privacy and the person(s) responsible for doing so.

Recommended Content Related to Logging and Monitoring Attendance at Privacy Training

- Requirement to maintain a log to track attendance of health information custodians and their agents at privacy training;
- Person(s) responsible for maintaining the log;
- Person(s) responsible and procedure for tracking attendance at privacy training, including identifying and ensuring health information custodians and their agents attend privacy training;
- The consequences for failing to attend privacy training.

Harmonized Privacy Assurance Policies and Procedures

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Recommended Content Related to Privacy Impact Assessments (PIAs)

- Circumstances in which a PIA is required to be conducted and in which a PIA is required to be reviewed and amended;
- Person(s) responsible for monitoring and identifying circumstances in which a PIA is required to be conducted or amended;
- Person(s) responsible for deciding whether a PIA must be conducted or amended and for conducting or amending a PIA;
- Content of a PIA and procedure for conducting or amending a PIA;
- Person(s) responsible for reviewing and approving a PIA and remediation plan and implementing and monitoring compliance with a remediation plan.

Recommended Content Related to Threat Risk Assessments (TRAs)

- Circumstances in which a TRA is required to be conducted and in which a TRA is required to be reviewed and amended;
- Person(s) responsible for monitoring and identifying circumstances in which a TRA is required to be conducted or amended;
- Person(s) responsible for deciding whether a TRA must be conducted or amended and for conducting or amending a TRA;
- Content of a TRA and procedure for conducting or amending a TRA;
- Person(s) responsible for reviewing and approving a TRA and remediation plan and implementing and monitoring compliance with a remediation plan.

Recommended Content Related to Privacy Readiness Assessments

- Person(s) responsible for establishing requirements to evaluate the privacy risks posed by electronic service providers and health information custodians and their agents;
- Person(s) responsible for setting risk ratings for each requirement;
- Person(s) responsible for creating, maintaining and administering the privacy readiness assessments;
- Requirement to complete the readiness assessments and to develop and implement the remediation plans for risks identified;
- Person(s) responsible for reviewing, approving and implementing readiness assessments and monitoring compliance with remediation plans.

Recommended Content Related to Ongoing Privacy Assurance

- Person(s) responsible for establishing requirements to evaluate the ongoing privacy risks posed by electronic service providers and health information custodians and their agents;
- Person(s) responsible for setting risk ratings for each requirement;
- What form will the assessment of the ongoing privacy risks take:
  - Will it include audits? If so, who will be responsible, what form will the audits take and how frequent will the audits be?
  - Will it include self-attestations? If so, who will be responsible for creating, maintaining, administering, reviewing and approving self-attestations and monitoring compliance with remediation plans?
  - What consequences will arise if no longer satisfy the requirements?

Recommendations Related to End User Agreements

- Require execution prior to accessing personal health information in the shared electronic system and every year thereafter;
- Set out the purposes for which personal health information may be collected, used and disclosed in the shared electronic system;
- Require health information custodians and their agents to acknowledge that they have read, understood and agree to comply with the policies and procedures for the shared electronic system;
- Require health information custodians and their agents to agree to comply with their duties and obligations under the *Act;*
- Set out the consequences for failing to comply; and
- Require notification if a privacy breach has or is about to occur.

Recommendations Related to Privacy Notice

- Require that prior to accessing personal health information in the shared electronic system, a notice be displayed that:
  - Sets out the purposes for which personal health information is permitted to be collected, used and disclosed;
  - Requires health information custodians and their agents to acknowledge they have read, understood and agree to comply with the applicable policies and procedures;
  - Requires health information custodians and their agents to agree to comply with their duties and obligations under the *Act;*
  - Sets out the consequences for failing to comply.

Harmonized Logging, Auditing and Monitoring Policies and Procedures

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Recommended Content for Auditing, Logging and Monitoring

- Set out events that will logged, audited and monitored, including:
  - Any time all or part of the personal health information in the shared electronic system is collected, used and disclosed;
  - A consent directive is made, withdrawn or modified;
  - A consent directive is overridden;
- Required content of each type of log;
- Person(s) responsible for logging, auditing and monitoring;
- To whom the logs may be provided upon request or otherwise;
- Auditing and monitoring criteria;
- Procedure if an actual or suspected privacy breach is identified.

Harmonized Consent Management Policies and Procedures

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Recommended Content Related to Obtaining Consent

- Meaning of “collect,” “use” and “disclose”;
- Purposes for which personal health information may be collected, used or disclosed in the shared electronic system;
- Type of consent required for the collection, use or disclosure;
- Person(s) responsible and the procedure for obtaining consent;
- Notice that will be provided to individuals;
- Manner in which the notice will be provided and its content;
- Person(s) responsible for implementation of the notice.

Recommended Content Related to Consent Directives

- Types of consent directives that an individual may request;
- Whether the consent directives apply only to the shared electronic system or to local systems as well;
- Person(s) responsible and procedure and timeframe for receiving and implementing consent directives and validating identity;
- Information provided to individuals requesting consent directives and person(s) responsible for providing the information;
- Person(s) responsible for testing consent directives;
- Those notified and the manner, timeframe, content and person(s) responsible for providing notice of consent directives.

Recommended Content Related to Consent Directive Overrides

- Purposes for which consent directives may be overridden;
- Duty to identify the purpose for the consent directive override;
- Purposes for which personal health information collected as a result of a consent directive override may be used or disclosed;
- Person(s) responsible and the procedure to be followed in logging, auditing and monitoring overrides of consent directives;
- The length of time a consent directive override will be in place;
- Those notified and the manner, timeframe, content and person(s) responsible for providing notice of overrides of consent directives.

Harmonized Privacy Breach Management Policies and Procedures

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Recommended Content Related to Identification of Breaches

- Meaning of a “privacy breach;”
- Duty on agents to notify the health information custodian on whose behalf they act of actual or suspected privacy breaches;
- Timeframe, manner and content of the notice that must be provided to the health information custodian;
- Person(s) responsible and the timeframe for determining whether a privacy breach occurred.

Recommended Content Related to Notification of Breaches

- Obligation to notify all health information custodians participating in the shared electronic system of actual privacy breaches;
- Timeframe, manner and content of the notice that must be provided to all participating health information custodians;
- Person(s) responsible for determining whether the privacy breach should be reported to any other person;
- Person(s) responsible for notifying affected individuals, i.e.:
  - The health information custodian where the breach occurred
  - The custodian where the individual most recently received health care
  - The custodian where the individual received the most health care
- The required content of the notice to affected individuals.

Recommended Content Related to Containment and Investigation

- Person(s) responsible for containment and investigation in circumstances where the privacy breach is caused by or involves:
  - A single health information custodian
  - Multiple custodians in one shared electronic system
  - Multiple custodians in multiple shared electronic systems
  - One or more third parties
- Timeframe within which an investigation report must be prepared and the required content of the investigation report;
- Person(s) who will be permitted to review and comment on the investigation report and to whom a final report must be submitted;
- Information that will be provided to affected individuals following an investigation of a privacy breach.

Recommended Content Related to Remediation

- Person(s) responsible for remediation of the privacy breach;
- Person(s) responsible for ensuring that measures to remediate the privacy breach have been implemented;
- Person(s) responsible and the timeframe and manner in which the status of implementation of measures to remediate the privacy breach are reported and to whom they are reported;
- Requirement to maintain a log of all privacy breaches and the required content of these logs;
- Person responsible for maintaining and for auditing and monitoring the log of privacy breaches to identify patterns and trends.

Harmonized Privacy Complaint & Inquiries Management Policies and Procedures

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Recommended Content Related to Inquiries

- Person(s) responsible for documenting, tracking, addressing and responding to a privacy inquiry where the inquiry relates to:
  - A single health information custodian
  - Multiple health information custodians
  - The entire shared electronic system
- Procedure and timeframe for logging and forwarding the inquiry, where applicable, and notifying the person making the inquiry;
- Timeframe within which an inquiry must be responded to;
- Person(s), if any, who will be permitted to review and comment on the response to the inquiry;
- Requirement to maintain a log of all inquiries.

Recommended Content Related to Complaints

- Person(s) responsible for documenting, tracking, remediating and responding to a privacy complaint where the complaint relates to:
  - A single health information custodian
  - Multiple health information custodians
  - The entire shared electronic system
- Procedure and timeframe for logging and forwarding the complaint, where applicable, and notifying the person making the complaint;
- Timeframe for determination of whether to investigate complaint and to whom notification of this determination must be provided.

Recommended Content Related to Complaints

- Timeframe within which an investigation report must be prepared and the required content of the investigation report;
- Person(s) who will be permitted to review and comment on the investigation report and to whom a final report must be submitted;
- Timeframe within which a complaint must be responded to and the required content of the response to the complaint;
- Person(s) who will be permitted to review and comment on the response to the complaint;
- Requirement to maintain a log of all complaints.

Harmonized Access and Correction Policies and Procedures

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Recommended Content Related to Requests for Access

- Person(s) responsible for responding to a request for access in circumstances where the request relates to records:
  - Created or contributed solely by one health information custodian
  - Created or contributed by more than one health information custodian
  - Collected by the health information custodian
- Person(s) responsible for responding to request for audit logs;
- Person(s) responsible for validating the identity of the individual;
- Procedure and timeframe for logging and forwarding the request, where applicable, and notifying the person making the request.

Recommended Content Related to Requests for Correction

- Person(s) responsible for responding to a request for access in circumstances where the request relates to records:
  - Created or contributed solely by one health information custodian
  - Created or contributed by more than one health information custodian
  - Collected by the health information custodian
- Person(s) responsible for validating the identity of the individual;
- Procedure and timeframe for logging and forwarding the request, where applicable, and notifying the person making the request;
- Requirement that shared electronic system maintains and displays a history of all corrections.