PROTECTING HEALTH INFORMATION IN AN ELECTRONIC ENVIRONMENT

Reaching Out to Ontario

- May 6, 2015

Debra Grant, Director of Health Policy

Manuela Di Re, Director of Legal Services

Information and Privacy Commissioner of Ontario

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

Why is the Protection of Privacy So Critical?

The need to protect the privacy of individuals' personal health information has never been greater given the:

- Extreme sensitivity of personal health information
- Greater number of individuals involved in the delivery of health care to an individual
- Increased portability of personal health information
- Emphasis on information technology and electronic exchanges of personal health information

The Promise of Electronic Records

- Potential to facilitate more efficient and effective health care and improve the quality of health care provided
- Accessible by all health care providers involved in the health care of an individual, regardless of location
- More complete than paper records which tend to be spread over a wide range of health care providers
- Easier to read and locate than paper records
- Can be designed to enhance privacy, i.e. through access controls, audit logs and strong encryption

The Peril of Electronic Records

- If privacy is not built into their design and implementation, electronic records pose unique risks to privacy
- Make it easier to transfer or remove personal health information from a secure location
- May attract hackers and others with malicious intent
- Increases the risk of authorized individuals accessing personal health information for unauthorized purposes

Consequences of Inadequate Attention to Privacy

If inadequate attention is paid to privacy, this may result in:

- Discrimination, stigmatization and psychological or economic harm to individuals based on the information
- Individuals being deterred from seeking testing or treatment
- Individuals withholding or falsifying information provided to health care providers
- Loss of trust or confidence in the health system
- Costs and lost time in dealing with privacy breaches
- Legal liabilities and ensuing proceedings

Potential Causes of Privacy Breaches

1. Lack of Clarity Regarding Responsibilities in Shared Systems

Challenges Posed by Shared Electronic Health Record Systems

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

How to Reduce the Risk …

A governance framework and harmonized privacy policies and procedures are needed to:

- Set out the roles and responsibilities of each participating health information custodian
- Set out the expectations for all health information custodians and agents accessing personal health information
- Ensure all health information custodians are operating under common privacy standards
- Set out how the rights of individuals will be exercised

Harmonized Privacy Policies and Procedures Needed

Harmonized privacy policies and procedures should address:

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

…Some Examples

Policy and Procedures Related to Privacy Training and Awareness

- Requirement to provide and attend initial and ongoing training
- Person(s) responsible for developing and implementing training
- Required minimum content of training materials
- Requirement to review and refresh training materials and the person(s) responsible and the frequency of this review
- Requirement to track attendance at training and the person(s) responsible and the procedure to be followed in this regard
- The consequences for failure to attend training
- Mechanisms to foster a culture of privacy

Fostering A Culture of Privacy – End User Agreements

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

Fostering A Culture of Privacy – Privacy Notices

Require that prior to accessing personal health information in the shared system, a notice be displayed that:

- Sets out the purposes for which personal health information is permitted to be collected, used and disclosed
- Requires end users to acknowledge they have read, understood and agree to comply with the policies and procedures and to agree to comply with their obligations under the *Act*
- Sets out the consequences for failure to comply

Policy and Procedures Related to Auditing, Logging and Monitoring

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

Policy and Procedures Related to Obtaining Consent

- Meaning of “collect,” “use” and “disclose”
- Purposes for which personal health information is permitted to be collected, used and disclosed
- Type of consent required for each collection, use and disclosure
- Person(s) responsible and the procedure for obtaining consent
- Notice that will be provided to individuals and the manner and content of the notice that will be provided
- Person(s) responsible for developing and implementing notice

Policy and Procedures Related to Consent Directives and Overrides

- Types of consent directives that may be requested and the systems in which the consent directives will be applied
- Purposes for which consent directives may be overridden and the length of time an override will be in place
- 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, procedure and timeframe to implement consent directives and to log, audit and monitor overrides

Policy and Procedures Related to Requests for Access and Correction

- Person(s) responsible for responding to requests 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 requests for audit logs
- Person(s) responsible for validating identity
- Procedure and timeframe to log and forward the request, where applicable, and to notify the person making the request
- Requirement to maintain and display history of all corrections

2. Increased Portability of Personal Health Information

Orders HO-004, HO-007 and HO-008

Our office has issued three orders involving personal health information on mobile and portable devices:

Order HO-004 – Theft of a laptop containing the unencrypted personal health information of 2,900 individuals

Order HO-007 – Loss of a USB containing the unencrypted personal health information of 83,524 individuals

Order HO-008 – Theft of a laptop containing the unencrypted personal health information of 20,000 individuals

How to Reduce the Risk….

- **STOP** and ask "Do I really need to store personal health information on this device?"
- **THINK** about the alternatives:
  - Would de-identified or coded information serve the purpose?
  - Could the information instead be accessed remotely through a secure connection or virtual private network?
- If you need to retain it on such a device, **PROTECT** it by:
  - Ensuring it is encrypted and protected with strong passwords
  - Retaining the least amount of personal health information
  - Developing policies and procedures, train and audit compliance

3. Unauthorized Access

Orders HO-002, HO-010 and HO-013

Our office has issued three orders involving unauthorized access:

Order HO-002

- A registered nurse accessed records of the estranged spouse of her boyfriend to whom she was not providing care
- They were accessed over six-weeks during divorce proceedings

Order HO-010

- A diagnostic imaging technologist accessed records of the current spouse of her former spouse to whom she was not providing care
- They were accessed on six occasions over nine months

Order HO-013

- Two employees accessed records to market and sell RESPs

Examples from Other Jurisdictions—Alberta

Investigation Report H2011-IR-004

- Physician used Alberta Netcare to view records of a partner's former spouse and mother and girlfriend of the former spouse
- Used the accounts of colleagues who failed to log out
- Viewed records on 21 occasions over a period of 15 months

Investigation Report Pending

- Pharmacist pleaded guilty and was fined $15,000
- Used Alberta Netcare to view the records of a number of women who attended her church and posted the prescription information of some of the women on Facebook

Examples from Other Jurisdictions—Saskatchewan

Investigation Report H-2010-001

- Pharmacist used the Pharmaceutical Information Program, a domain repository in Saskatchewan's electronic health record, to view drug profiles of three individuals on nine occasions after a business arrangement with the individuals dissolved

Investigation Report H-2013-001

- Employees of Regina Qu'Appelle Regional Health Authority viewed their own health information, viewed and modified the health information of other employees and viewed the health information of other individuals

Examples from Other Jurisdictions – Manitoba

Report 2011-0513 and 2011-0514

- An employee of CancerCare Manitoba viewed the electronic medical record of a child of an acquaintance
- The employee viewed three tabs – patient notes, agenda and summary – for two minutes two seconds
- Because the record was created earlier that day, the employee was only able to view the name and cancer registry number

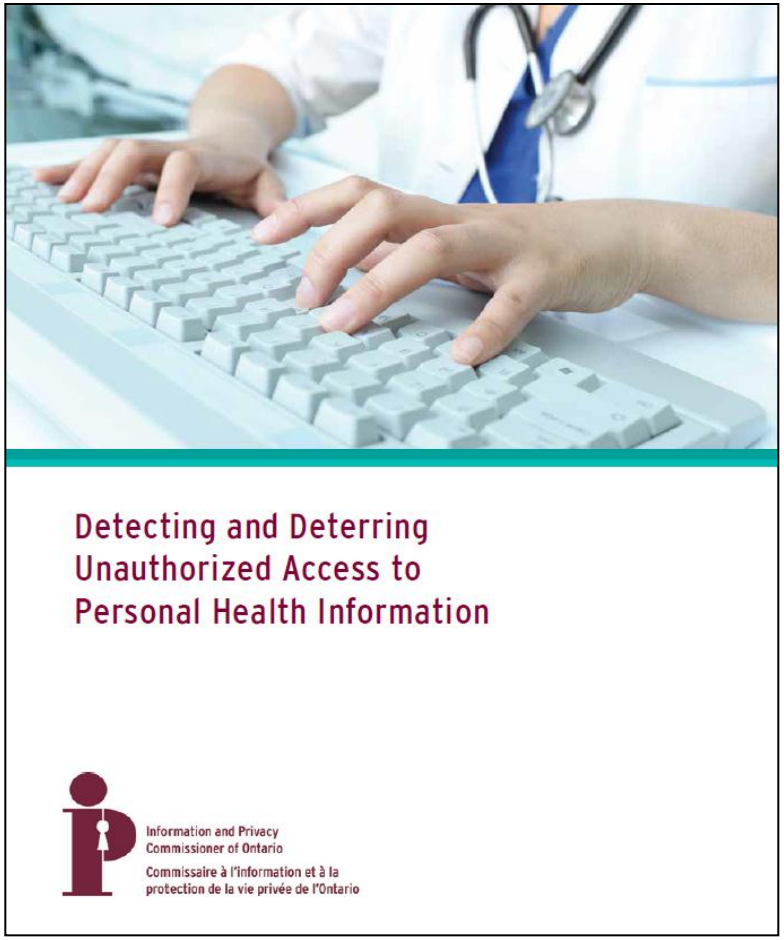
Examples from Other Jurisdictions – Newfoundland and Labrador

- A clerk at Western Health inappropriately viewed the records of 1,043 individuals between June 2011 and May 2012
- An employee of Central Health inappropriately viewed records of an individual more than twenty times over seven years
- Eleven employees at Eastern Health inappropriately viewed the records of more than 100 individuals
  - Five employees were terminated (a licensed practical nurse, two clerks and two nurses) and six others were suspended

How to Reduce the Risk…

- Clearly articulate the purposes for which employees, staff and other agents may access personal health information
- Provide ongoing training and use multiple means of raising awareness such as:
  - Confidentiality and end-user agreements
  - Privacy notices and privacy warning flags
- Immediately terminate access pending an investigation
- Implement appropriate access controls and data minimization
- Log, audit and monitor access to personal health information
- Impose appropriate discipline for unauthorized access

New Guidance Document: Detecting and Deterring Unauthorized Access

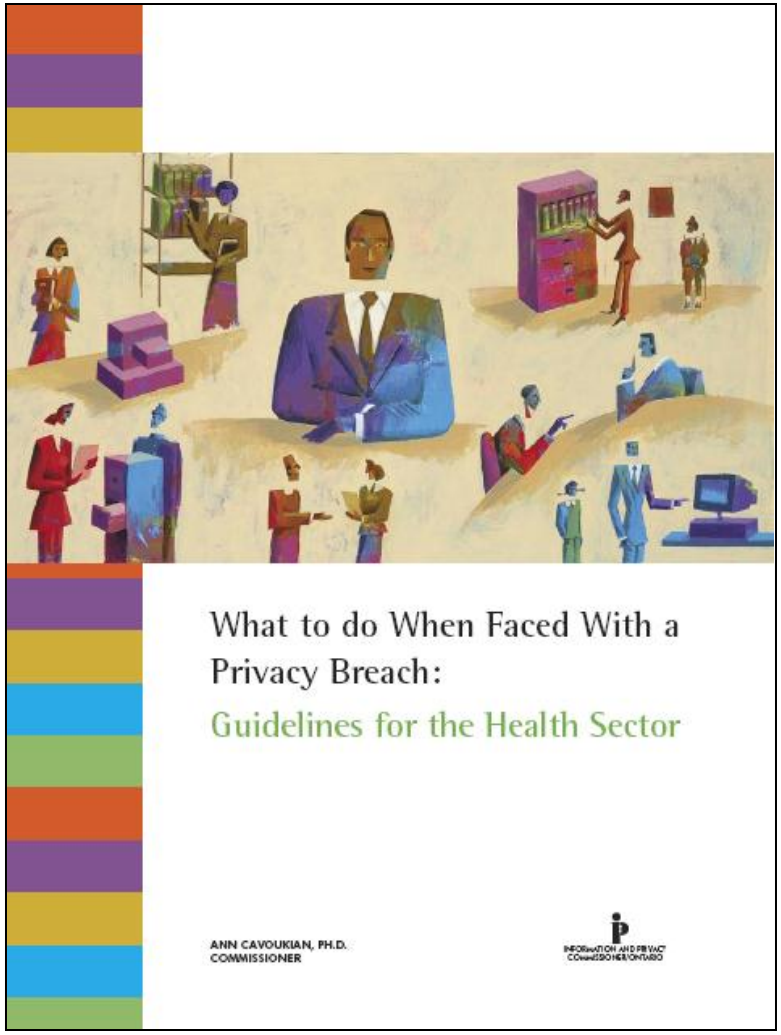


- Impact of unauthorized access
- Reducing the risk through:
  - ✓ Policies and procedures
  - ✓ Training and awareness
  - ✓ Privacy notices and warning flags
  - ✓ Confidentiality and end-user agreements
  - ✓ Access management
  - ✓ Logging, auditing and monitoring
  - ✓ Privacy breach management
  - ✓ Discipline

Planning for a Privacy Breach

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

Develop and Implement a Privacy Breach Management Protocol



Privacy Breach Protocol – Identification of Breaches

- Define a “privacy breach”
- Impose duty on agents to notify the health information custodian of actual or suspected privacy breaches
- Set out the timeframe, manner and content of the notice that must be provided to the health information custodian
- Identify the person(s) responsible and the timeframe for determining whether a privacy breach occurred

Privacy Breach Protocol – Breach Notification

- Require notification of all health information custodians participating in the shared system of actual breaches
- Set out the timeframe, manner and content of the notice that must be provided to all participating custodians
- Identify the person(s) responsible for determining whether the breach should be reported to any other person
- Identify person(s) responsible for notifying affected individuals:
  - 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
- Set out required content of the notice to affected individuals

Privacy Breach Protocol – Containment and Investigation

- Identify the person(s) responsible for containment and investigation where the privacy breach is caused by or involves:
  - A single health information custodian
  - Multiple custodians in one shared system
  - Multiple custodians in multiple shared systems
  - One or more third parties
- Set out the timeframe within which an investigation report must be prepared and the required content of the report
- Identify the person(s) who will review and comment on the investigation report and who will receive a final report
- Set out information that will be provided to affected individuals

Privacy Breach Protocol – Remediation

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

How to Contact Us

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca