Debra Grant
Director of Health Policy, IPC
&
Manuela Di Re
Director of Legal Services, IPC

# Protecting Health Information in an Electronic Environment

Reaching Out to Ontario
Queen's University, Kingston
May 4, 2016

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

www.ipc.on.ca

# 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

Inadequate attention to privacy 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

# *Bill 119*
# *Health Information Protection Act, 2015*

# Overview

- The Bill was introduced on September 16, 2015 and has been ordered for third reading
- The Bill proposes to:
  - Require privacy breaches to be reported to our office and to relevant regulatory colleges
  - Remove the requirement that prosecutions be started within six months of when the offence occurred
  - Double fines for offences from $50,000 to $100,000 for individuals and $250,000 to $500,000 for organizations

# Summary of Provisions Related to the Provincial Electronic Health Record

- Bill 119 will only apply to the provincial electronic health record (Provincial EHR) and not to electronic medical record systems or shared electronic health record systems

- In relation to the provincial EHR, the Bill will:
  - Set out rules for the collection, use and disclosure of personal health information
  - Establish processes by which individuals can implement consent directives with respect to their personal health information
  - Establish processes by which individuals can access their records of personal health information

# Rules for Collection, Use and Disclosure

- In general, health information custodians can only collect personal health information from the provincial EHR:
  - To provide or assist in the provision of health care to the individual to whom the information relates, or
  - If have reasonable grounds to believe it is necessary to eliminate or reduce a significant risk of serious bodily harm
  - If collected to provide or assist in provision of health care, it may be used or disclosed for any purpose permitted by *PHIPA*
  - If collected to prevent a significant risk of serious bodily harm, it may only be used and disclosed for this purpose

# Consent Directives and Overrides

- Individuals will have the right to implement a directive to withhold or withdraw consent to the collection, use or disclosure of their information for health care purposes
- The individual must submit the directive to a prescribed organization that is responsible for implementing the directive
- Health information custodians can override a directive:
  - With express consent
  - If reasonable grounds to believe it is necessary to eliminate or reduce a significant risk of serious bodily harm to the individual or another person, but if to the individual must also establish not reasonably possible to get timely consent

# Consent Directives and Overrides

- Personal health information collected through an override may only be used or disclosed for the purpose it was collected
- Consent overrides will be audited and monitored and written notice of the override will be immediately provided to the health information custodian who collected the information
- The health information custodian must then notify the individual of the consent override and, in certain circumstances, must also notify the Commissioner

# 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* (*PHIPA*)

# How to Reduce the Risk …

- As Bill 119 will not apply to shared electronic health record systems, 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 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 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 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. Unauthorized Access

# Meaning of Unauthorized Access

- When you view, handle or otherwise deal with personal health information without consent and for purposes not permitted by *PHIPA*, for example:
  - When not providing or assisting in the provision of health care to the individual; and
  - When not necessary for the purposes of exercising employment, contractual or other responsibilities
- The act of viewing personal health information on its own, without any further action, is an unauthorized access

# Examples of Unauthorized Access – Education and Quality Improvement

- There have been a number of instances where agents have accessed personal health information claiming it was for:
  - Their own educational purposes
  - To improve the quality of the health care they provide
  - Other uses permitted by *PHIPA*
- Demonstrating this access is unauthorized is often difficult

# Challenges in Establishing "Unauthorized" Access

- Demonstrating such accesses are unauthorized may be difficult where the custodian does not:
  - Have clear policies specifying the purposes for which access is and is not permitted
  - Have procedures that must be followed when accessing information for purposes other than providing care
  - Inform agents what access is permitted and is not permitted, including through training, notices, flags, agreements, etc.

# Consequences of Unauthorized Access

- Review or investigation by privacy oversight bodies
- Prosecution for offences
- Statutory or common law actions
- Discipline by employers
- Discipline by regulatory bodies

# 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

# Offences

- It is an offence to wilfully collect, use or disclose personal health information in contravention of *PHIPA*
- The Attorney General is responsible for commencing prosecutions for offences under *PHIPA*
- Anyone may refer a matter to the Attorney General
- On conviction, an individual may be liable to a fine of up to $50,000 and a corporation of up to $250,000
- These fines will be doubled when Bill 119 comes into effect

# Referrals for Prosecution

To date, five matters have been referred for prosecution

**2011**

- A nurse at North Bay Health Centre

**2015**

- Radiation therapists at the University Health Network

**2015**

- A social worker at a family health team

**2016**

- A registration clerk at a regional hospital

**2016**

- A regulated professional at a Toronto hospital

# Examples from Other Jurisdictions—Alberta

**Prosecution in 2007**

- A medical office clerk plead guilty and was fined $10,000 under the *Health Information Act*
- Accessed the information of the wife of a man with whom she was having an affair using Alberta Netcare and fax
- Accessed the information on six different occasions

**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

# Examples from Other Jurisdictions—Alberta

**Investigation Report Pending**

- Pharmacist plead guilty and was fined $15,000 under the *Health Information Act*
- 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

**Prosecution in 2014**

- A medical laboratory assistant received a four month conditional sentence, eight months probation and a $500 fine
- Accessed the personal health information of 34 individuals and uttered forged documents under the *Criminal Code*

# 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

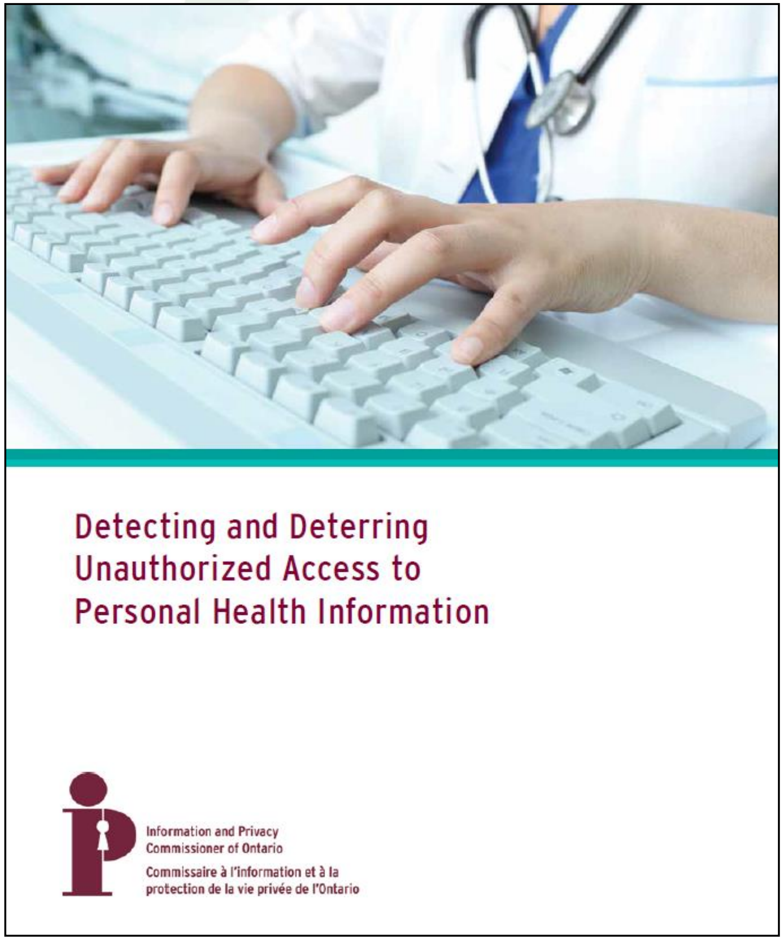
**Investigation Report H-2013-001**

- 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

# 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



Detecting and Deterring Unauthorized Access to Personal Health Information

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

- 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

# *Emerging Issue of Ransomware*

# What is Ransomware?

- A type of malware installed on a device or system
- Starts by tricking a user to install malicious software on a personal or work computer, usually in the form of a spam email sent in the form of an invoice, website or video
- When the user opens the attachment, the software encrypts the hard drive or specific files and locks the user out, making the data inaccessible until the user pays a ransom to the malware operators to regain access
- Ransom is usually requested in Bitcoin

# Ransomware at Hollywood Presbyterian Medical Center

- In February 2016, the Hospital was infiltrated by malware that left it without access to digital patient records, some internet-connected medical devices and email for nearly two weeks

- The hospital paid a ransom of 40 bitcoins or about $16,900 to get the decryption key to restore its systems

- The hackers originally demanded over $3 million

- The hospital insisted there was no evidence that the hackers accessed patient records

# Ransomware – the Ontario Experience

- In March 2016, the Ottawa Hospital confirmed that four of its computers were hit with ransomware

- The ransomware encrypted information on the computers making it inaccessible to hospital administrators

- A spokesperson indicated that "no patient information was obtained through the attempt."

# Ransomware – the Ontario Experience

- In March 2016, it was reported that the website of Norfolk General Hospital was hacked and ransomware was installed on the website during the attack
- A security researcher reported the website was pushing ransomware to computers that visited the website
- Norfolk General Hospital confirmed three of its computers were infected with ransomware and that the computers were restored from backups and no ransom paid

# How to Reduce the Risk …

- Educate agents to only download email attachments or click on links from trusted sources
- Avoid opening any email attachments that are unsolicited
- Back-up all personal health information regularly
- Test back ups to ensure they are working as expected
- Ensure security software and anti-virus are current
- Configure internet security software to receive automatic malware notices and perform real-time malware scans

# Advisory for Ransomware

## What is Ransomware?

Ransomware is malicious software (malware) installed on your device or system, including smartphones and tablets, that encrypts the hard drive or specific files then demands a ransom be paid before the device or information is decrypted. Importantly, hackers may access your data during the course of an attack.

Ransomware is typically spread via phishing where an attachment or link in an email or text message contains malware that is installed when opened. Ransomware on one device may spread to other devices through network vulnerabilities.

Variations of ransomware exist to attack most operating systems, including Windows, Android and iOS (Apple). Publicized instances of ransomware have occurred at hospitals and media organizations, as well as thousands of personal devices. There are several types of ransomware that you can learn more about online.

## Preventive Measures

Alberta's privacy laws require reasonable steps be taken to protect against risks to personal or health information. The OIPC recommends public bodies, health custodians and private sector organizations consider the following:

- Educate about phishing attacks. In particular, only download email attachments or click on links from trusted sources.
- Back up information and system files regularly, and test backups to ensure they are working as expected.
- Install internet security software and maintain updates.
- Configure internet security software to receive automatic malware notices and perform real-time malware scans, in addition to regularly scheduled malware scans.
- Install security patches for operating systems as soon as they become available.
- Bookmark trusted websites and access those websites via bookmarks.
- Avoid using administrator accounts for general use on your device. Administrator accounts that are exploited by malware may cause more damage.
- Ensure a breach response plan is in place and educate users about what to do if attacked.

## Ransomware Response

The severity of the attack and the safeguards you have in place will impact your response. Generally, the following actions are recommended:

- Disconnect the affected device or system from the rest of the network and from the internet.
- Run anti-malware scans in an attempt to identify and remove the ransomware, if possible.
- If you are able to restore your files or system from backup, you do not need to submit to a ransom demand.
- Review the response plan and update, as appropriate.
- Further education on preventive measures.

If a breach of personal information has occurred:

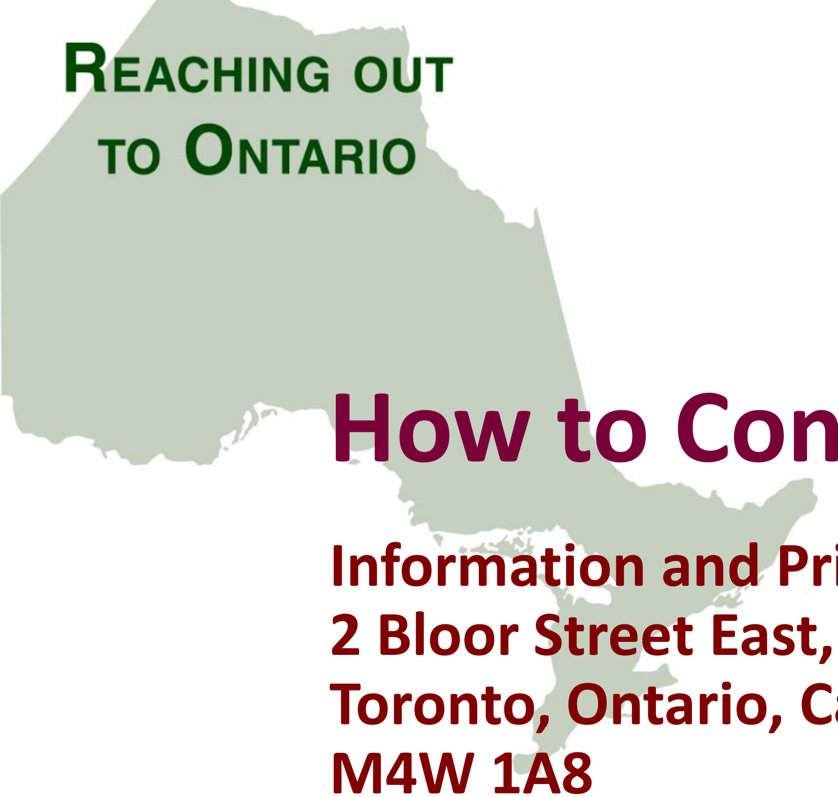
- Private sector organizations must consider if the intrusion presents a real risk of significant harm. If it does, under the *Personal Information Protection Act*, private sector organizations in Alberta must report the breach to the OIPC and may be required to notify affected individuals.
- Public bodies and health custodians are not required to report such incidents to the OIPC but are encouraged to contact the OIPC for advice and consider notifying affected individuals.

This document is an administrative tool intended to assist in understanding the *Freedom of Information and Protection of Privacy Act* (FOIP Act), *Health Information Act* (HIA) and *Personal Information Protection Act* (PIPA). This document is not intended as, nor is it a substitute for, legal advice. For the exact wording and interpretation of the FOIP Act, HIA or PIPA, please read the Acts and regulations in their entirety. This document is not binding on the Office of the Information and Privacy Commissioner of Alberta.

Office of the Information and
Privacy Commissioner of Alberta

www.oipc.ab.ca

MARCH 2016



# 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

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965