# PROTECTING PERSONAL HEALTH INFORMATION

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

Reaching Out to Ontario - Windsor

November 30, 2017

# Topics

1. Email Communications
2. Abandoned records
3. Fees for access
4. Bill 119 – *Health Information Protection Act, 2016*
5. Unauthorized access

# Email Communications

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

Fact Sheet

# Communicating Personal Health Information by Email

September 2016

Email is one of the dominant forms of communication today. Individuals and organizations have come to rely on its convenience, speed and economy for both personal and professional purposes. Health information custodians (custodians) are no exception. While email offers many benefits, it also poses risks to the privacy of individuals and to the security of personal health information. It is important for custodians to understand these risks and take steps to mitigate them before using email in their professional communications.

## OBLIGATIONS UNDER THE PERSONAL HEALTH INFORMATION PROTECTION ACT

The *Personal Health Information Protection Act* establishes rules for protecting the privacy of individuals and the confidentiality of their personal health information, while at the same time facilitating effective and timely health care. Custodians have a duty to ensure that health records in their custody or control are retained, transferred and disposed of in a secure manner. They are also required to take reasonable steps to protect personal health information against theft, loss and unauthorized use or disclosure.

## UNDERSTANDING THE RISKS

Like most forms of communication, email entails an element of risk. An email can be inadvertently sent to the wrong recipient, for example, by mistyping an email address or using the autocomplete feature. Email is often accessed on portable devices, such as smart phones, tablets and laptops, which are vulnerable to theft and loss. An email can also be forwarded or changed without the knowledge or permission of the original sender. Email may also be vulnerable to interception and hacking by unauthorized third parties.

Personal health information is sensitive in nature. Its unauthorized collection, use or disclosure may have far-reaching consequences for individuals, including stigmatization, discrimination and psychological harm. For custodians and their agents, privacy breaches may result in disciplinary proceedings, prosecutions and lawsuits. In addition, such privacy breaches may result in a loss of trust and confidence in the entire health sector that was entrusted to protect this sensitive information.

# Communicating by Email

- The *Personal Health Information Protection Act* (*PHIPA*) sets out rules for protecting the privacy of patients and the confidentiality of their personal health information (PHI), while facilitating effective and timely care
- Any communication of PHI involves risk, but communicating PHI by email has its own set of unique risks
- These risks must be considered by health information custodians (custodians) and their agents in order to protect the privacy and confidentiality of patients

# Technical, Physical and Administrative Safeguards

- Custodians are required to implement technical, physical and administrative safeguards to protect PHI
- Technical safeguards include:
  - encrypting portable devices
  - strong passwords
  - firewalls and anti-malware scanners
- Physical Safeguards:
  - restricting access by locking server rooms where email is retained
  - keeping portable devices in secure location

# Technical, Physical and Administrative Safeguards

- Administrative safeguards:
  - notice in emails that information is confidential
  - providing instructions for when email is received in error
  - communicate by professional vs personal accounts
  - confirming recipient email address is current
  - checking that email address is typed correctly
  - restricting access to email system and content on need-to-know basis
  - informing individuals of email changes
  - acknowledging receipt of emails
  - recommending that recipients implement these safeguards

# Email Between Custodians

- The IPC expects emailing of PHI among custodians to be secured by use of encryption
- There may be exceptional circumstances where communication of PHI between custodians through encrypted email may not be practical (i.e. in urgent circumstances where the PHI is needed to minimize a significant risk of serious bodily harm)
- Custodians should look to their regulatory colleges for applicable guidelines, standards or regulations

# Email Between Custodians and Patients

- Where feasible, custodians should use encryption for communicating with their patients
- Where not feasible, custodians should consider whether it is reasonable to communicate through unencrypted email.
  - Are there alternative methods?
  - Is the PHI urgently needed to minimize a significant risk of serious bodily harm?
  - Would the patient expect you to communicate with him/her in this manner?
  - How sensitive is the PHI to be communicated?
  - How much and how frequently will be PHI be communicated?

# Policy, Notice and Consent

## Policy

- Custodians are expected to develop and implement a written policy for sending and receiving PHI by email

## Notice and Consent

- Custodians are expected to notify their patients about this policy and obtain their consent prior to communicating by means of email that is not encrypted
- Consent may be provided in verbally or in writing

# Data Minimization, Retention and Disposal

## Data Minimization

- Custodians have a duty to limit the amount and type of PHI included in an email

## Retention and Disposal

- Custodians are required to retain and dispose of PHI in a secure manner
- PHI must only be stored on email servers and portable devices for as long as is necessary to serve the intended purpose

# Training and Privacy Breach Management

## Training and Education

- Comprehensive privacy and security training is essential for reducing the risk of unauthorized collection, use and disclosure of PHI

## Privacy Breach Management

- Custodians are expected to have a privacy breach management protocol in place that identifies the reporting, containment, notification, investigation and remediation of actual and suspected privacy breaches

# Abandoned Records

# Abandoned Records

- Since *PHIPA* came into effect, the IPC has investigated numerous instances of abandoned health records
- This typically occurs when a custodian relocates, retires, becomes incapacitated or otherwise ceases to practice
- Despite the legislative requirements to safeguard PHI in the custody or control of a custodian, records of PHI continue to be abandoned
- No entity or person has the authority to assume custody and control of abandoned records
- This may lead to privacy breaches, patients not being able to exercise their right of access, and health care providers not have accurate and complete information for health care purposes

# Previous Guidance

- In 2007, the IPC issued guidance on how to avoid abandoned records
  - *How to Avoid Abandoned Records: Guidelines on the Treatment of Personal Health Information, in the Event of a Change in Practice*
  - *Checklist for Health Information Custodians in the Event of a Planned or Unforeseen Change in Practice*
- The guidance focused on what to do in the event of a change in practice

# How to Avoid Abandoned Records

- Who is the Custodian in the Event of a Change in Practice?
- What Obligations are Imposed on Custodians in the Event of a Change in Practice?
- What are Best Practices in the Event of a Change in Practice?



Information and Privacy Commissioner/ Ontario

How to Avoid Abandoned Records: Guidelines on the Treatment of Personal Health Information, in the Event of a Change in Practice

# Ongoing Challenges

- Custodians are not being proactive, and records are being left behind or disposed of in an unsecure manner
- It may be difficult to identify or locate the custodian
- There may be no plan for transferring custody and control if the practitioner becomes incapacitated or dies
- There may be no plan for ongoing retention of records when a practitioner retires or relocates to another jurisdiction

# Jurisdictional Scan – Codes of Conduct

- Some regulatory colleges have included the requirement for members to notify the college before they leave or move their practice in their policies and codes of conduct
- Notification must include the location and disposition of records and a named successor who will provide continued access to the records
- Some regulatory colleges have made the abandonment of health records an act of professional misconduct

# Jurisdictional Scan – Amendments to Health Privacy Law

- Some jurisdictions supplemented the initiatives of regulatory colleges with amendments to their health privacy legislation
- Saskatchewan amended its *Health Information Protection Act* to authorize the Ministry of Health to appoint a person to act in place of a former trustee who abandoned records
- Additionally, abandoning records in Saskatchewan is now subject to a liability offence of up to $50,000 for individuals
- Saskatchewan includes a reverse onus clause – this means trustees must demonstrate that they took reasonable steps to prevent the abandonment of the records

# Jurisdictional Scan – Amendments to Laws Governing Providers

- Some jurisdictions supplemented the initiatives of regulatory colleges with amendments to legislation governing providers
- Manitoba amended its *Regulated Health Professions Act*
- This amendment has not yet been proclaimed
- When proclaimed, the College will be permitted to appoint a member to take over the responsibility of securing the records or apply to the Court to designate a custodian
- Members of each college will have a duty to ensure that their records are not abandoned
- Members who abandon health records will be guilty of an offence and liable to a fine up to $50,000

# Potential Solutions

- Policy Solutions
  - education and awareness
  - amendments to regulatory colleges policies and procedures
  - amendments to professional codes of conduct
- Legislative Solutions
  - amendments to health privacy legislation
  - Amendments to legislation governing health professionals

# Fees

# Fees for Collecting, Using and Disclosing Records

- *PHIPA* includes rules about fees that may be charged for collecting, using and disclosing records of PHI
- Section 35 of *PHIPA* states:
  - A health information custodian shall not charge a person a fee for collecting or using personal health information except as authorized by the regulations made under this Act.
  - When disclosing personal health information, a health information custodian shall not charge fees to a person that exceed the prescribed amount or the amount of reasonable cost recovery, if no amount is prescribed.

# Fees for Access to Records

- *PHIPA* includes rules about fees that may be charged for providing individuals with access to their own records
- Section 54 of *PHIPA* states, in part:
  - A health information custodian that makes a record of personal health information or a part of it available to an individual under this Part or provides a copy of it to an individual may charge the individual a fee for that purpose if the custodian first gives the individual an estimate of the fee
  - The amount of the fee shall not exceed the prescribed amount or the amount of reasonable cost recovery, if no amount is prescribed
  - A health information custodian may waive the payment of all or any part of the fee that an individual is required to pay if, in the custodian's opinion, it is fair and equitable to do so

# Reasonable Cost Recovery

- Since no amounts for fees have been prescribed in the regulations, custodians are not permitted to charge an amount that exceeds reasonable cost recovery
- In Orders HO-009 and HO-014, the IPC provided guidance on interpreting “reasonable cost recovery”

# Order HO-009 and HO-014

- For the purposes of subsections 35(2) and 54(11), the amount of the fee that may be charged shall not exceed $30 for any or all of the following:
  - receipt and clarification, if necessary, of a request for a record
  - providing an estimate of the fee that will be payable under subsection 54(10) in connection with the request
  - locating and retrieving the record
  - reviewing the contents of the record for not more than 15 minutes to determine if it contains PHI to which access or disclosure may or shall be refused
  - preparation of a response letter
  - preparation of the record for photocopying, printing or transmission

# Order HO-09 and HO-014 (Cont'd)

- photocopying the record to a maximum of the first 20 pages or printing the record to a maximum of the first 20 pages, excluding the printing of photographs stored in electronic form
- packaging the photocopied or printed copy of the record for shipping or faxing
- electronically transmitting a copy of the electronic record instead of printing and shipping or faxing the printed copy
- cost of faxing a copy of the record to a fax number in Ontario or mailing a copy by ordinary mail to an address in Canada
- supervising examination of the original record for not more than 15 minutes.
- additional fees that may be charged are set out in a chart

# Bill 119 – *Health Information Protection Act*

# Bill 119

- Bill 119 was introduced on September 16, 2015
- It amends *PHIPA*, including by introducing Part V.1
- Part V.1 relates to the provincial electronic health record (provincial EHR)
- All the provisions in the Bill were proclaimed into force on June 3, 2016, with the exception of those related to the provincial EHR

# Governance Model

- No custodian will have sole custody or control of PHI in the provincial EHR – it will be shared
- A custodian will only have custody or control of PHI if it:
  - creates and contributes the PHI to the provincial EHR, and
  - collects the PHI from the provincial EHR
- An advisory committee will be established to make recommendations to the Minister
- The Minister will establish membership of the committee, its terms of reference, organization and governance

# Responsibility for Developing and Maintaining the Provincial EHR

- The provincial EHR will be developed and maintained by one or more prescribed organizations
- The prescribed organization(s) will be required to comply with certain requirements, including:
  - logging, auditing and monitoring instances where PHI is viewed, handled or otherwise dealt with
  - logging, auditing and monitoring instances where consent directives are made, withdrawn, modified and overridden
  - having and complying with practices and procedures that are approved by the Commissioner every three years

# Collection, Use and Disclosure

- In general, custodians will only be permitted to collect PHI from the provincial EHR:
  - to provide or assist in the provision of health care to the individual to whom the PHI relates, or
  - if a custodian has reasonable grounds to believe it is necessary to eliminate or reduce a significant risk of serious bodily harm
- If PHI is collected to provide health care, it may subsequently 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
- Special definitions of collection, use and disclosure will apply

# Directed Disclosures

- The Minister will be able to direct the disclosure of PHI contributed by more than one custodian:
  - to prescribed registries (e.g. Cardiac Care Network of Ontario) for the purposes of section 39(1)(c) of *PHIPA*
  - to prescribed entities (e.g. Cancer Care Ontario) for the purposes of section 45 of *PHIPA*
  - to certain public health authorities (e.g. medical officers of health) for the purposes of section 39(2) of *PHIPA*
  - for research purposes in accordance with section 44 of *PHIPA*
- Prior to directing the disclosure, the Minister must submit the request received to and must consult with the advisory committee

# Consent Directives

- Individuals cannot opt out of having their PHI included in the provincial EHR
- Once included, however, individuals will have the right to implement consent directives
- A consent directive withholds or withdraws the consent of an individual to the collection, use or disclosure of his or her PHI for health care purposes
- Authority is provided to make regulations specifying the data elements that may not be subject to a directive

# Consent Overrides

- A custodian will be permitted to override a directive:
  - with the express consent of the individual; and
  - where there are 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 the risk is to the individual, it must not be reasonably possible to get timely consent
- A custodian that collects PHI subject to a directive may only use it for the purpose for which it was collected
- For example, where PHI is collected with express consent, it may only be used in accordance with the individual's consent

# Notice of Consent Overrides

- Where a directive is overridden, the prescribed organization will be immediately required to provide written notice to the custodian that collected the PHI
- Upon receipt of the notice, the custodian is required to:
  - notify the individual to whom the PHI relates at the first reasonable opportunity; and
  - where the PHI is collected to eliminate or reduce a significant risk of serious bodily harm to a third person, provide additional written notice to the Commissioner

# Breach Notification

- A custodian must notify the individual at the first reasonable opportunity if PHI in its custody or control is stolen, lost or used or disclosed without authority
- In the context of the provincial EHR, the custodian must also notify the individual at the first reasonable opportunity if PHI is collected without authority
- The Commissioner must also be notified if the circumstances surrounding the theft, loss or unauthorized collection, use or disclosure meets certain prescribed requirements

# Breach Notification to the Commissioner

- Regulations prescribing when the Commissioner must be notified came into force October 1, 2017

- The IPC recently published a guidance document explaining when a breach must be reported to the Commissioner

SEPTEMBER 2017

## Reporting a Privacy Breach to the Commissioner

GUIDELINES FOR THE HEALTH SECTOR

To strengthen the privacy protection of personal health information, the Ontario government has amended the *Personal Health Information Protection Act* (the act). Under section 12(3) of the act and its related regulation, custodians must notify the Information and Privacy Commissioner of Ontario (the Commissioner) about certain privacy breaches. This law takes effect **October 1, 2017**.

As a custodian, you must report breaches to the Commissioner in seven categories described in the regulation and summarized below. The categories are not mutually exclusive; more than one can apply to a single privacy breach. If at least one of the situations applies, you must report it. The following is a summary—for the complete wording of the regulation, see the appendix at the end of this document.

It is important to remember that even if you do not need to notify the Commissioner, you have a separate duty to notify individuals whose privacy has been breached under section 12(2) of the act.

### SITUATIONS WHERE YOU MUST NOTIFY THE COMMISSIONER OF A PRIVACY BREACH

**1. Use or disclosure without authority**

This category covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian. An example would be where a

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

# Circumstances Where a Breach Must be Reported to the Commissioner

- A custodian has reasonable grounds to believe that PHI in its custody or control was:
  - **used or disclosed without authority by a person who knew or ought to have known that they were using or disclosing the information without authority**
    - The person could be your employee, a health care practitioner with privileges, a third party (such as a service provider), or even someone with no relationship to you
    - Typical example is the "snooping case"
    - You generally do not need to notify the Commissioner when the breach is accidental, for example, when information is inadvertently sent by email or courier to the wrong person
    - However, accidental privacy breaches must be reported if fall into one of the other categories
  - **stolen**
    - An example is where someone has stolen paper records or a laptop or other electronic device
    - You do not need to notify the Commissioner if the information was de-identified or properly encrypted

# Circumstances Where a Breach Must be Reported to the Commissioner (Cont'd)

- **after an initial loss or unauthorized use or disclosure, the PHI was or will be further used or disclosed without authority**
  - An example is where an agent accessed PHI without authority and subsequently used this information to market products or services or to commit fraud (such as health care or insurance fraud)
  - Even if you did not report the initial incident, you must notify the Commissioner of this situation
- **loss or unauthorized use or disclosure is part of a pattern of similar losses or unauthorized uses or disclosures of PHI**
  - An example is you discover that a letter to a patient inadvertently included PHI relating to a different patient. Over a few months, the same mistake is repeated several times because an automated process for generating letters has been malfunctioning for some time
  - You must use your judgment in deciding if a privacy breach is an isolated incident or part of a pattern
  - Take into account, for instance, the time between the breaches and their similarities
  - Keeping track of privacy breaches in a standard format will help you identify patterns.

# Circumstances Where a Breach Must be Reported to the Commissioner (Cont'd)

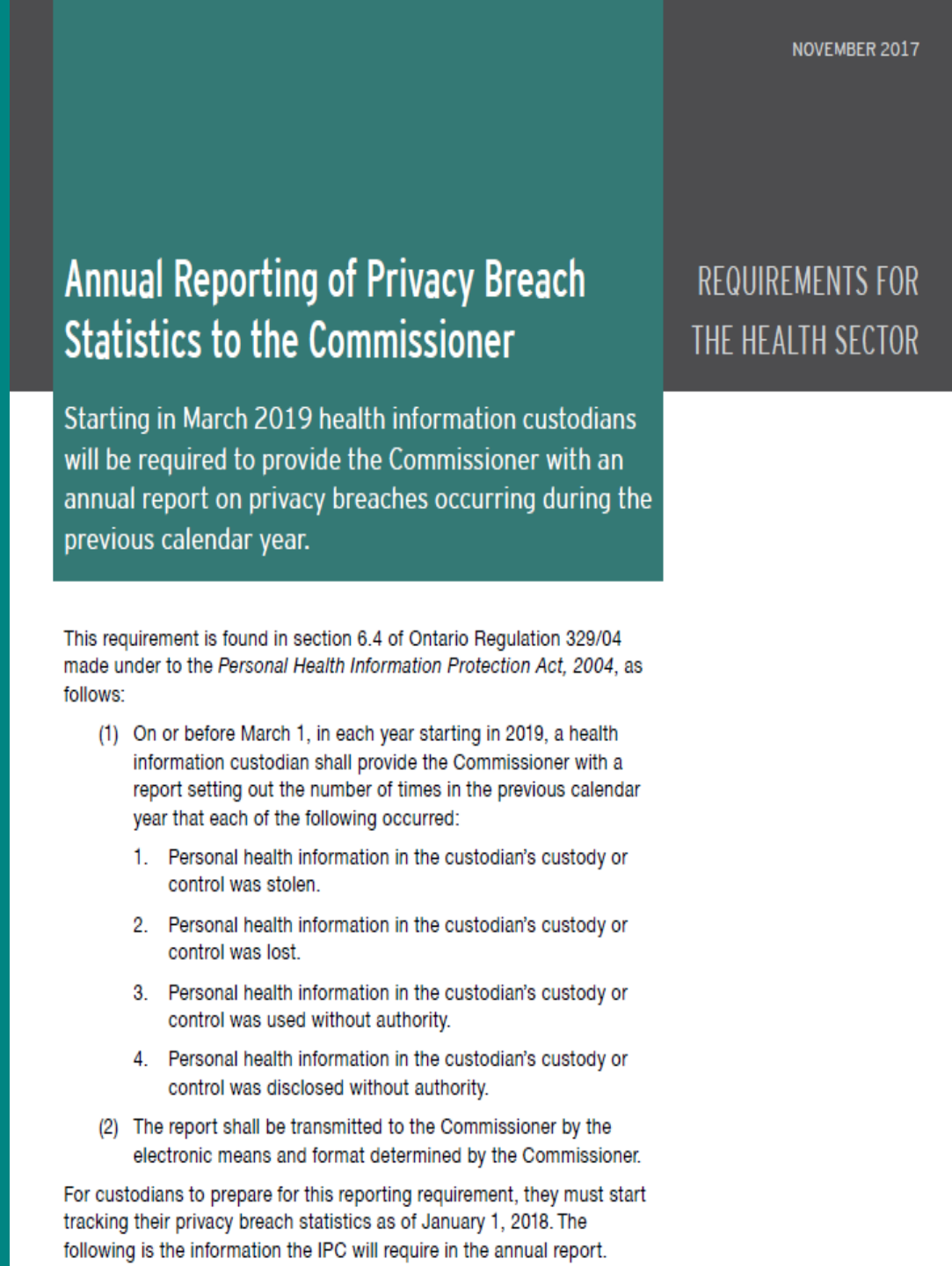
- **A custodian is required to give notice to a College of an event described in section 17.1 of *PHIPA* that relates to a loss or unauthorized use or disclosure of PHI**
  - Custodians must give notice to a health regulatory college of an event described in section 17.1 of PHIPA
  - Custodians must also give notice to the Commissioner of losses or unauthorized uses and disclosures in the same circumstances a custodian is required to give notice to a health regulatory college under section 17.1
  - Where an agent is a member of a health regulatory college, you must notify the Commissioner of a loss or unauthorized use or disclosure of PHI if:
    - you terminate, suspend or discipline them as a result of the breach
    - they resign and you believe this action is related to the breach
  - Where a health care practitioner with privileges or otherwise affiliated with you is a member of a college, you must notify the Commissioner of a loss or unauthorized use or disclosure of PHI if :
    - you revoke, suspend or restrict their privileges or affiliation as a result of the breach
    - they relinquish or voluntarily restrict their privileges or affiliation and you believe this is related to the breach

# Circumstances Where a Breach Must be Reported to the Commissioner (Cont'd)

- A custodian would be required to give notice to a College, if an agent of the custodian were a member of the College, of an event described in section 17.1 of the *PHIPA* that relates to a loss or unauthorized use or disclosure of PHI
  - Not all agents of a custodian are members of a college
  - If an agent is not a member, you must still notify the Commissioner in the same circumstances that would have triggered notification to a college, had the agent been a member
- A custodian determines the loss or unauthorized use or disclosure of PHI is significant after considering all relevant circumstances, including whether:
  - the PHI that was lost or used or disclosed without authority is sensitive
  - the loss or unauthorized use or disclosure involved a large volume of PHI
  - the loss or unauthorized use or disclosure involved many individuals' PHI
  - more than one custodian or agent was responsible for the loss or unauthorized use or disclosure of the PHI

# Annual Reports to the Commissioner

- Custodians will be required to:
  - start tracking privacy breach statistics as of January 1, 2018
  - provide the Commissioner with an annual report of the previous calendar year's statistics, starting in March 2019.
- The IPC recently released a guidance document on this statistical reporting requirement



NOVEMBER 2017

## Annual Reporting of Privacy Breach Statistics to the Commissioner

REQUIREMENTS FOR THE HEALTH SECTOR

Starting in March 2019 health information custodians will be required to provide the Commissioner with an annual report on privacy breaches occurring during the previous calendar year.

This requirement is found in section 6.4 of Ontario Regulation 329/04 made under to the *Personal Health Information Protection Act, 2004*, as follows:

(1) On or before March 1, in each year starting in 2019, a health information custodian shall provide the Commissioner with a report setting out the number of times in the previous calendar year that each of the following occurred:

1. Personal health information in the custodian's custody or control was stolen.
2. Personal health information in the custodian's custody or control was lost.
3. Personal health information in the custodian's custody or control was used without authority.
4. Personal health information in the custodian's custody or control was disclosed without authority.

(2) The report shall be transmitted to the Commissioner by the electronic means and format determined by the Commissioner.

For custodians to prepare for this reporting requirement, they must start tracking their privacy breach statistics as of January 1, 2018. The following is the information the IPC will require in the annual report.

# Unauthorized Access

# Meaning of Unauthorized Access

- When you view, handle or otherwise deal with PHI 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 PHI 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 PHI claiming it was for:
  - their own educational purposes
  - to improve the quality of the health care they provide
  - other uses permitted by *PHIPA*
- 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.

# Examples of Unauthorized Access – Health Professionals with Privileges

- Agents may have off-site practices where they, and their staff, have access to PHI on the custodian's electronic information system
- For example, a doctor with privileges at a hospital may operate a clinic where he or she employs administrative staff and this staff may have access to the hospital's information system
- Where this doctor employs staff with access to PHI in the custody or control of the hospital, both the doctor and hospital are responsible for the activities of the staff

# Health Professionals with Privileges

- The roles of the hospital, doctor and doctor's staff should be specified, in a written agreement, to clarify who is:
  - a custodian,
  - an agent of the hospital, and
  - an agent of the health professional
- The agreement should also clarify who is responsible for ensuring there is appropriate training, that confidentiality agreements are signed, that policies and procedures are followed, 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 PHI in contravention of *PHIPA*
- Consent of the Attorney General is required to commence a prosecution for offences under *PHIPA*
- On conviction, an individual may be liable to a fine of up to $100,000 and a corporation of up to $500,000

# Prosecutions

To date, six individuals have been prosecuted:

- **2011**– A nurse at North Bay Health Centre
- **2016**– Two radiation therapists at a Toronto Hospital
- **2016** – A registration clerk at a regional hospital
- **2017** – A social worker at a family health team
- **2017**– An administrative support clerk at a Toronto hospital

# Successful Prosecutions – Two Radiation Therapists

- The two radiation therapists were charged with wilfully collecting, using or disclosing PHI in contravention of *PHIPA*
- The two radiation therapists pled guilty to wilfully using PHI in contravention of *PHIPA*
- Each was fined $2,000
- These were the first successful prosecutions under *PHIPA*

# Successful Prosecutions – Registration Clerk

- The registration clerk was charged with one count of collecting, using or disclosing PHI contrary to *PHIPA*
- The registration clerk pled guilty
- She was ordered to pay a $10,000 fine and a $2,500 victim surcharge

# Successful Prosecution – Social Worker

- A Masters of Social Work student, who was on an educational placement with a family health team in Central Huron pled guilty to willfully accessing the PHI of five individuals
- As part of her plea, she agreed she accessed the PHI of 139 individuals without authorization between September 2014 and March 2015
- She was ordered to pay a $20,000 fine and a $5,000 victim surcharge
- This is the highest fine to date for a health privacy breach in Canada

*"The various victims have provided victim impact statements which are quite telling in terms of the sense of violation, the loss of trust, the loss of faith in their own health care community, and the utter disrespect [the accused] displayed towards these individuals."*

*"I have to take [the effect of deterrence on the accused] into consideration, but realistically, it's general deterrence, and that has to deal with every other heath care professional or someone who is governed by this piece of legislation. This is an important piece of legislation …"*

- Justice of the Peace, Anna Hampson

# Successful Prosecutions – Administrative Support Clerk

- The administrative support clerk pled guilty to one count of willfully using PHI contrary to *PHIPA* in relation to 44 individuals
- She printed the PHI of 28 of these individuals
- She was ordered to pay a $8,000 fine a $2,000 victim surcharge

# How to Reduce the Risk…

- Clearly articulate the purposes for which employees, staff and other agents may access PHI
- 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 PHI
- Impose appropriate discipline for unauthorized access

# 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

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

# 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