Protecting Personal Health Information

Association of Family Health Teams of Ontario
June 26, 2017

Fida Hindi, Health Law Counsel
Office of the Information and Privacy Commissioner of Ontario

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

Outline

- The *Personal Health Information Protection Act* (the *Act* or *PHIPA*)
  - Application of the *Act*
  - Email communications
  - Unauthorized access
  - Bill 119, *Health Information Protection Act, 2016*
  - Mandatory breach reporting

APPLICATION OF THE *ACT*

Application of the Act

- The *Personal Health Information Protection Act, 2004* came into force on November 1, 2004 (the *Act*)
- The majority of the *Act* governs "personal health information" (PHI) in the custody or control of:
  - "Health Information Custodians," or
  - "Agents" of health information custodians
- However, the *Act* also has broader application
- For example it contains restrictions on the use and disclosure of PHI by non-custodians that receive PHI from custodians

Definition of Personal Health Information

Defined as identifying information about an individual in oral or recorded form that:

- Relates to an individual's physical or mental health
- Relates to the provision of health care to the individual
- Identifies an individual's health care provider
- Identifies an individual's substitute decision-maker
- Relates to payments or eligibility for health care
- Is the individual's health number
- Is a plan of service under the *Home Care and Community Services Act, 1994* for the individual
- Relates to the donation of body parts or bodily substances

Definition of Health Information Custodian

Health information custodians include:

- A health care practitioner who provides health care
- A person who operates a group practice of health care practitioners who provide health care
- A hospital, psychiatric facility and independent health facility
- A pharmacy, ambulance service, laboratory or specimen collection centre
- A long-term care home, care home or home for special care
- A community care access corporation
- A medical officer of health of a board of health
- Minister/Ministry of Health and Long-Term Care
- Minister/Ministry of Health Promotion

Definition of Agent

- An agent is a person that, with the authorization of a custodian, acts for or on behalf of the custodian in respect of PHI

- It is irrelevant whether or not the agent:
  - is employed by the custodian
  - is remunerated by the custodian
  - has the authority to bind the custodian

- A custodian remains responsible for PHI collected, used, disclosed, retained or disposed of by an agent

Duties Imposed on Health Information Custodians and Their Agents

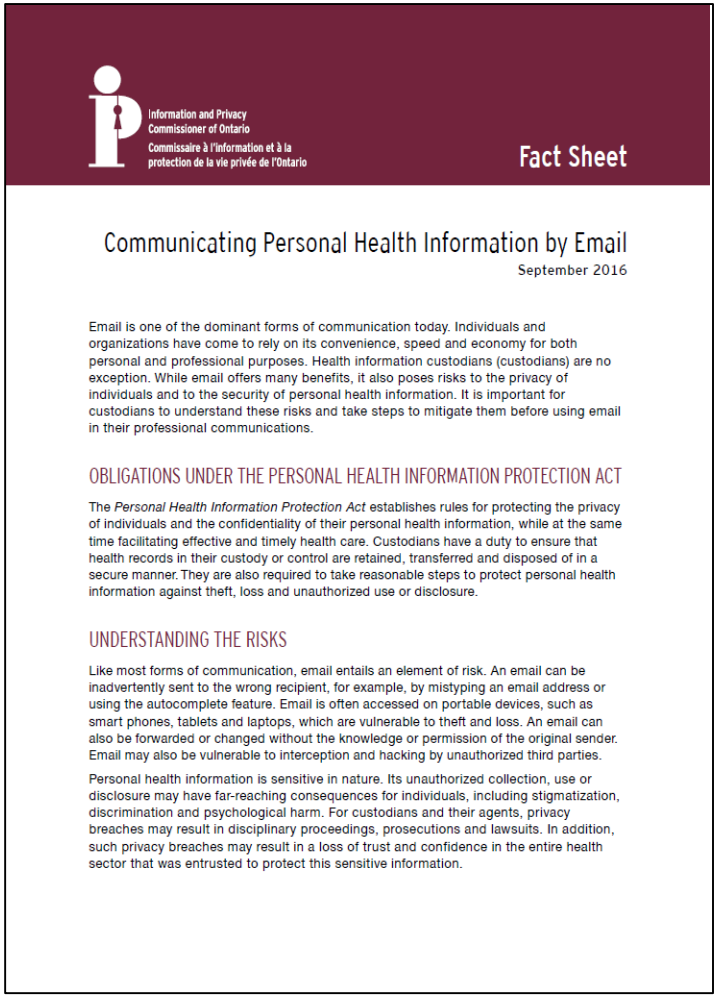
- A number of duties are imposed on custodians and their agents under the *Act*

- These duties generally fall into four categories:
  - Collection, use and disclosure of PHI
  - Security of PHI
  - Responding to requests for access to and correction of records of PHI
  - Transparency of information practices

Email Communications

Fact Sheet: Communicating PHI by Email

- Describes the risks of using email and custodians' obligations under *PHIPA*
- Outlines technical, physical and administrative safeguards needed to protect PHI and the policies, procedures and training custodians should have in place
- Difference between custodian-to-custodian and custodian-to-patient 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.

Technical, Physical & Administrative Safeguards

- Custodians are required to implement technical, physical and administrative safeguards to protect PHI in email
- Technical safeguards include:
  - Encrypting portable devices
  - Strong passwords
  - Firewalls and anti-malware scanners
- Physical Safeguards:
  - Restricting access where equipment used to send/receive PHI by email is kept
  - Keeping portable devices in secure location (locked drawer/cabinet)

Technical, Physical & 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

Communicating PHI by Email – *Between Custodians*

- For emailing PHI between custodians, IPC expects encryption, barring exceptional circumstances

- Custodians should look to their regulatory colleges for applicable guidelines, standards or regulations

Communicating PHI by Email – *Custodians and Patients*

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

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

Communicating PHI by Email – *Cont'd*

- Data minimization principle applies, even with patient consent: custodian has a duty to limit the amount and type of PHI included in an email.
- Custodians have obligation to retain and dispose of emails containing PHI in a secure manner.
  - only retain emails containing PHI as long as necessary to serve purpose; avoid duplication on email servers and portable devices when email already documented in patient record
  - encrypt portable devices
  - provide agents with initial and ongoing privacy and security training, including on email policy
  - have a privacy breach management protocol in place

Unauthorized Access

Meaning of Unauthorized Access

- When you view, use, disclose, 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

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

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

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

Damages for Breach of Privacy - PHIPA

- Person affected by Commissioner's order or by conduct that gave rise to a conviction of an offence under PHIPA may commence a proceeding in the Superior Court of Justice
- Claim for damages for actual harm suffered as a result of contravention of PHIPA or as a result of the conduct
- Limit of $10,000 for mental anguish

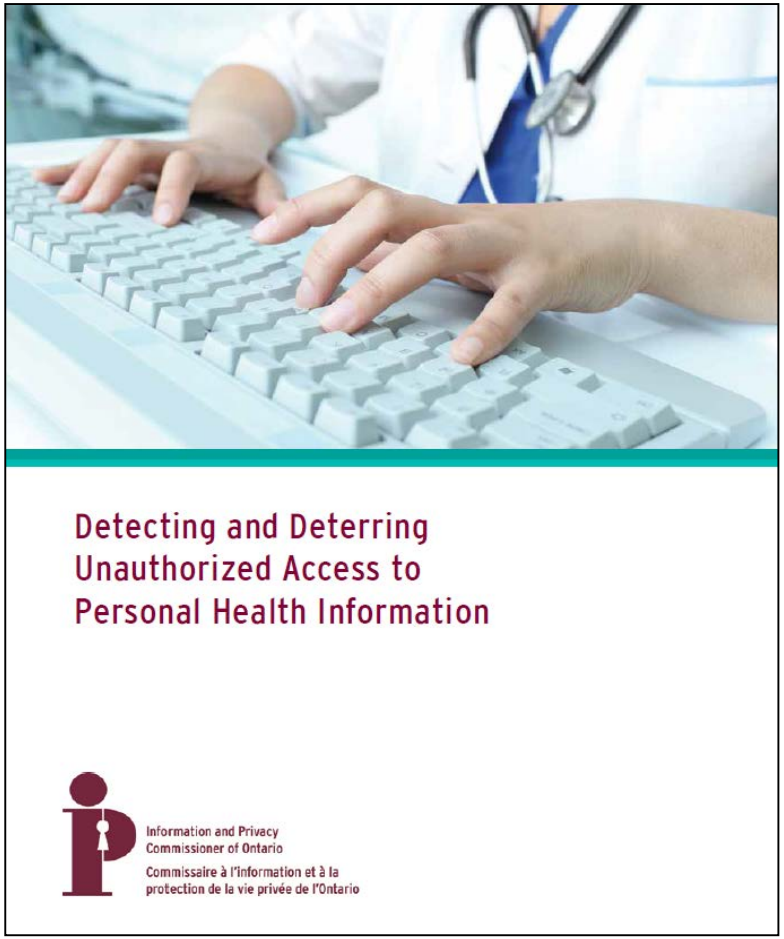
Jones v. Tsige, 2012 ONCA 32

- In 2012, the Ontario Court of Appeal recognized a new cause of action for "intrusion upon seclusion"
- Under this new cause of action, the plaintiff must prove that:
  - The defendant's conduct was intentional
  - The defendant invaded, without lawful justification, the plaintiff's private affairs or concerns, and
  - A reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish
- Proof of actual loss is not required for an award of damages under this tort
- Court of Appeal capped damages at $20,000 where there is no pecuniary loss

Detecting and Reducing the Risk of Unauthorized Access

- Clearly articulate the purposes for which employees, staff and other agents may access PHI
- Provide initial and ongoing training
- 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

Bill 119 – *Health Information Protection Act, 2016*

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 to the provincial EHR, and
  - collects 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 Electronic Health Record

- 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 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 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
    - Must include in notice a statement that individual is entitled to make a complaint to the Commissioner
- The Commissioner must also be notified if the circumstances surrounding the theft, loss or unauthorized use or disclosure meets certain prescribed requirements

Breach Notification

- 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 by means of the EHR
    - Must include in notice a statement that individual is entitled to make a complaint to the Commissioner
- In the context of the provincial EHR, the Commissioner must also be notified if the circumstances surrounding the unauthorized collection meet certain prescribed requirements

Breach Notification

- The Minister posted a proposed regulation in March 2017 on the prescribed requirements
- Comment period on the proposed regulation is now closed
- The proposed regulation can be found in the Ontario Gazette and on Ontario's Regulatory Registry
- Not proclaimed

Notification to Regulatory Colleges

- Custodian must provide written notice to the College within 30 days where a health care practitioner who is a member of a College that the custodian employs:
  - is terminated, suspended or subject to disciplinary action as a result of the unauthorized collection, use, disclosure, retention or disposal of PHI by the employee
  - resigns and the custodian has reasonable grounds to believe that the resignation is related to an investigation or other action by the custodian with respect to an alleged unauthorized collection, use, disclosure, retention or disposal of PHI by the employee

Notification to Regulatory Colleges

- If a custodian extends privileges to, or is otherwise affiliated with, a health care practitioner who is a member of a College, the custodian must give written notice within 30 days of:
  - the member's privileges being revoked, suspended or restricted, or his or her affiliation being revoked, suspended or restricted, as a result of the unauthorized collection, use, disclosure, retention or disposal of PHI by the member
  - the member relinquishing or voluntarily restricting his or her privileges or his or her affiliation and the custodian has reasonable grounds to believe that this is related to an investigation or other action by the custodian with respect to an alleged unauthorized collection, use, disclosure, retention or disposal of PHI by the member

DISCLAIMER

This presentation is provided for informational purposes and is not legal advice. The information provided on Bill 119 is subject to change as the regulations have not been proclaimed.