Electronic Communication of Personal Health Information

Laura Crestohl

Senior Health Policy Advisor

Information and Privacy Commissioner of Ontario

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

InnomarLive 2018 – Healthcare Innovation

October 4th, 2018

Cont'd

Agenda

- Protecting Privacy when Communicating Electronically
- Communicating Personal Health Information (PHI) by Email
- Unauthorized Access

Protecting Privacy When Communicating Electronically

Protecting Privacy when Communicating PHI Electronically

- The need to protect the privacy of individuals' personal health information (PHI) has never been greater given the:
  - Extreme sensitivity of PHI
  - Number of individuals involved in the delivery of health care to an individual
  - Increased portability of PHI
  - Emphasis on information technology and electronic exchanges of PHI

Cont'd

Consequences of Inadequate Attention to Privacy

- 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 practitioners
- Loss of trust or confidence in the health case system
- Costs and lost time in dealing with privacy breaches
- Legal liabilities and ensuing proceedings

Cont'd

Security of Records of PHI and Data Minimization

Regardless of the means of communication personal health information…

Security of Personal Health Information

- The *Personal Health Information Protection Act* (PHIPA) requires records of PHI to be retained, transferred and disposed of in a secure manner
- Custodians must take reasonable steps in the circumstances to ensure:
  - PHI is protected against theft, loss and unauthorized use or disclosure
  - Records of PHI are protected against unauthorized copying, modification and disposal

Data Minimization

- Custodians must not collect, use or disclose:
  - PHI if other information will serve the purpose
  - More PHI than is reasonably necessary to meet the purpose

Communicating PHI by Email

Communicating PHI by Email

- PHIPA sets out rules for protecting the privacy of individuals and the confidentiality of their PHI while at the same time facilitated effective and timely care.

- Any communication of PHI involves risk, but communicating PHI by email has its own set of unique risks that must be considered by health information custodians and their agents in order to protect the privacy of individuals and the confidentiality of their records of PHI.

Technical, Physical & Administrative Safeguards

- Under PHIPA, 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** include:
  - Restricting access by locking server rooms where email is retained
  - Keeping portable devices in secure location

Cont'd

Technical, Physical & Administrative Safeguards

- **Administrative Safeguards** include:
  - 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 a need-to-know basis
  - Informing individuals of email changes
  - Acknowledge receipt of emails
  - Recommending that recipients implement these safeguards

Email Between Custodians

- The IPC expects emailing of PHI between custodians to be secured by the use of encryption
- There may be exceptional circumstances where communication of PHI between custodians through encrypted email may not be practical (eg: in emergencies)
- Custodians should look to their health regulatory colleges for applicable guidelines, standards or regulations

Email Between Custodians & Patients

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

Policy, Notice & 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 via email that is not encrypted
- Consent may be provided verbally or in writing

Data Minimization, Retention & Disposal of PHI

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 should only be stored on email servers and portable devices for as long as is necessary to serve the intended purpose

Training & Privacy Breach Management

Training and Education

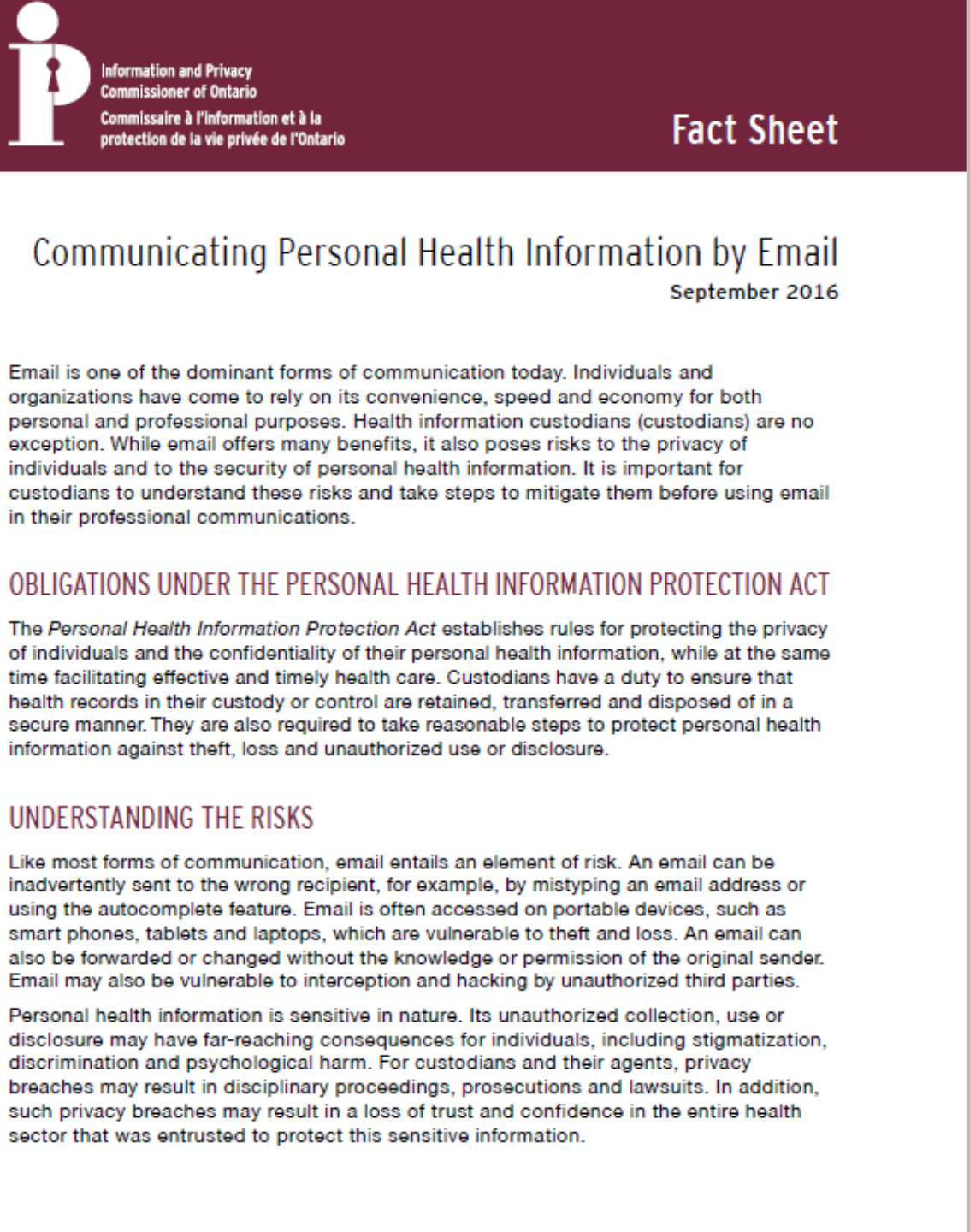
- Comprehensive privacy and security training is essential for reducing the risk of unauthorized collection, use and disclosure of PHI

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

Communicating PHI by Email

- Obligations under PHIPA
- Understanding and addressing the risks including:
  - Safeguards
  - Policy, notice and consent
  - Data minimization
  - Retention and disposal of PHI
  - Training
  - Privacy Breach Management



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.

Unauthorized Access

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, even without any further action, is an unauthorized access

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 willfully 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

Referrals for Prosecution

To date, six individuals have been referred for prosecution

- 2011 – a nurse at North Bay Health Centre
- 2016 – two radiation therapists at the University Health Network
- 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

Reducing the Risk of Unauthorized Access

- 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

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

Questions?

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