# Electronic Communication of Personal Health Information

A presentation to the Porcupine Health Unit
(Timmins, Ontario)
May 11th, 2017

*Nicole Minutti, Health Policy Analyst*

Information and Privacy
Commissioner of Ontario

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

# Agenda

1. Protecting Privacy when Communicating Electronically
2. Communicating PHI by Email
3. Electronic Health Records and Bill 119
4. Mobile Devices
5. Unauthorized Access
6. Ransomware

# Protecting Privacy when Communicating PHI Electronically

- The need to protect the privacy of individuals’ personal health information has never been greater given the:
  - Extreme sensitivity of personal health information
  - 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

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

# Security of Records of PHI & Data Minimization

*Regardless of the means of communicating personal health information…*

## Security of PHI

- 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

# Agenda

1. Protecting Privacy when Communicating Electronically
2. Communicating PHI by Email
3. Electronic Health Records and Bill 119
4. Mobile Devices
5. Unauthorized Access
6. Ransomware

# Communicating PHI by Email

- The *Personal Health Information Protection Act* sets out rules for protecting the privacy of individuals and the confidentiality of their personal health information (PHI), while at the same time facilitates 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 their patients and the confidentiality of their records of personal health information.

# Technical, Physical & Administrative Safeguards

- Under PHIPA, custodians are obligated to implement technical, physical and administrative safeguards to protect the PHI of their patients.
- Technical Safeguards:
  - Encrypting portable devices
  - Strong passwords
  - Firewalls and anti-malware scanners
- Physical Safeguards:
  - Restricting access, locking rooms where email is sent
  - Keeping portable devices in secure location

# 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

# Email Among 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 (e.g. emergencies)
- Custodians should look to their health regulatory colleges for applicable guidelines, standards or regulations on the use of unencrypted email to communicate PHI.

# 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 it an emergency?
  - Would the patient expect you to communicate with him or her in this way?
  - 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 via email that is not encrypted
- Consent may be provided in verbally or in writing

# Data Minimization, Retention and Disposal of PHI

## Data Minimization

- Custodians have a duty to limit the amount and type of personal health information 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 and Privacy Breach Management

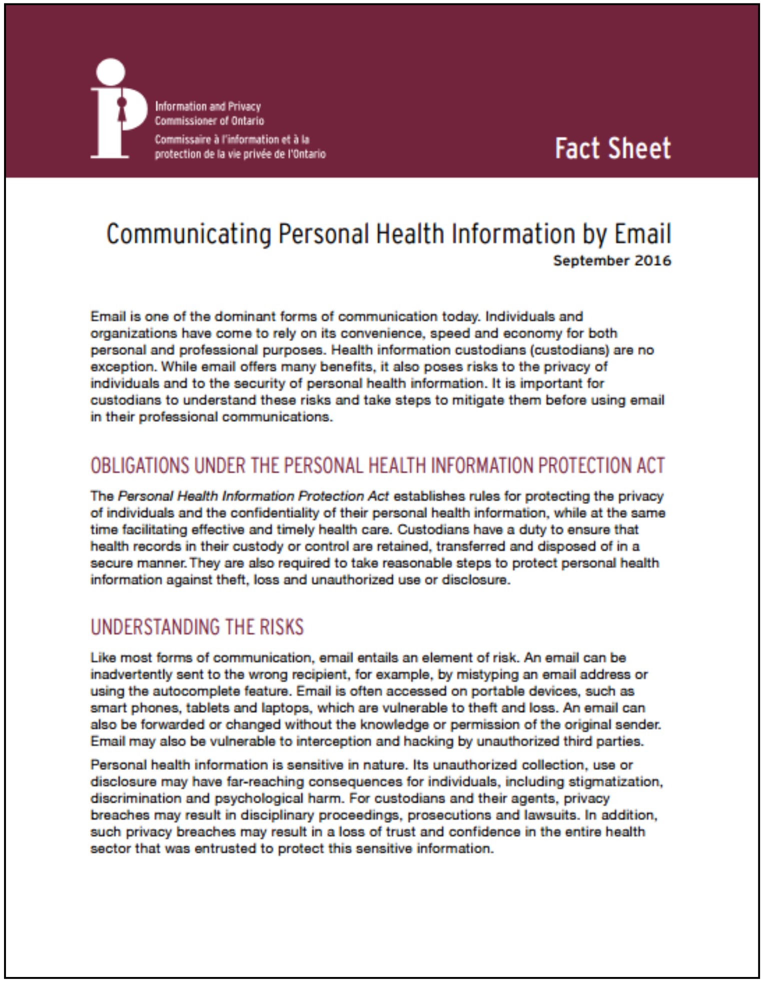
## Training & Education

- 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

# Guidance from the IPC: Communicating PHI by Email



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.

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

# Agenda

1. Protecting Privacy when Communicating Electronically
2. Communicating PHI by Email
3. Electronic Health Records and Bill 119
4. Mobile Devices
5. Unauthorized Access
6. Ransomware

# The Promise of Electronic Health 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 Health Records

- If privacy is not built into their design and implementation, electronic health 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

# Bill 119: Proclaimed Provisions

## Proclaimed provisions

- Definition of “use” has been clarified to include “viewing” of personal health information
- New provision requires custodians to take steps that are reasonable in the circumstances to ensure PHI is not collected without authority
- Requires prescribed types of privacy breaches to be reported to our office and to relevant regulatory colleges
- Removes the requirement that prosecutions be started within 6 months of when the offence occurred
- Doubles the fines for offences from $50,000 to $100,000 for individuals and $250,000 to $500,000 for organizations

# Bill 119: Provisions Not Yet Proclaimed

## Provisions not yet proclaimed

- Provisions related to the provincial electronic health record (EHR)
- These provisions will:
  - Set out the rules for the collection, use and disclosure of personal health information in a provincial EHR
  - 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 from the provincial EHR

# Agenda

1. Protecting Privacy when Communicating Electronically
2. Communicating PHI by Email
3. Electronic Health Records and Bill 119
4. Mobile Devices
5. Unauthorized Access
6. Ransomware

# Mobile Devices

- Mobile devices may be especially vulnerable to loss, theft, or accessed by unauthorized individuals
- If it is necessary to retain personal health information on mobile devices:
  - Only retain the minimal amount of personal health information and for the minimal amount of time necessary
  - Ensure personal health information is strongly encrypted
  - Ensure the encryption keys are not stored with or on the device
  - Ensure the use of strong password protection
- Develop a policy and procedures for secure retention on mobile or portable devices
  - Provide training to agents on the policy and procedures,
  - Regularly audit compliance with the policy and procedures,
  - Regularly review the policy and procedures

# Agenda

1. Protecting Privacy when Communicating Electronically
2. Communicating PHI by Email
3. Electronic Health Records and Bill 119
4. Mobile Devices
5. Unauthorized Access
6. Ransomware

# 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

# 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

# Referrals for Prosecution

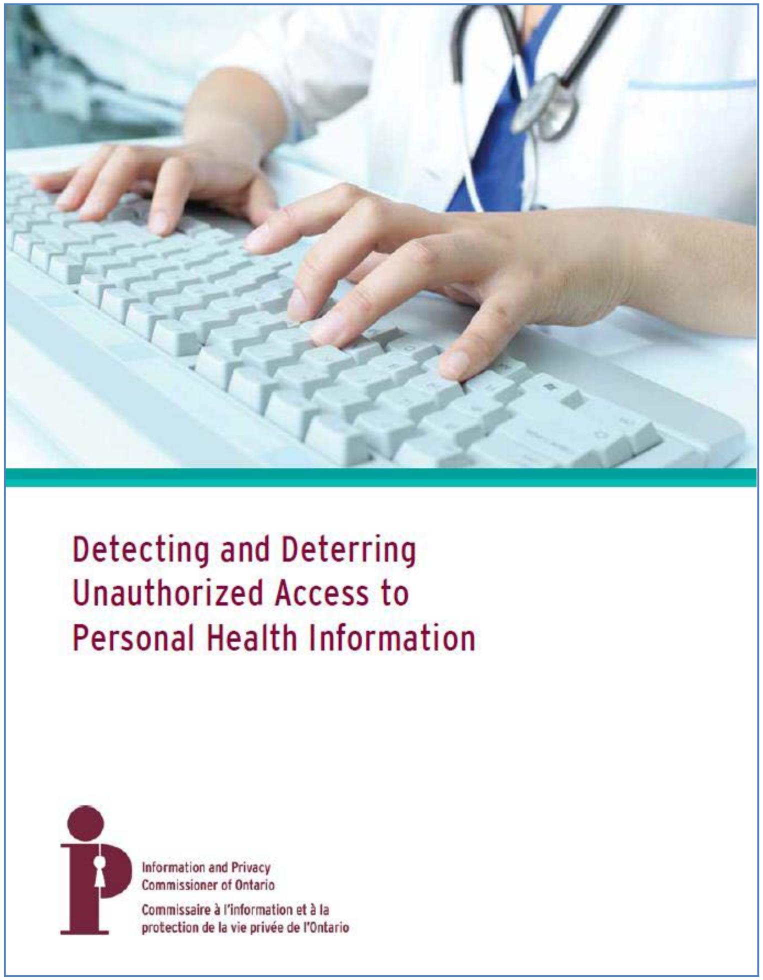
To date, six individuals have been referred for prosecution

- **2011** – a nurse at North Bay Health Centre
- **2015** – two 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

# Reducing the Risk of Unauthorized Access

- 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

# Guidance from the IPC: 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

Reduce risk through:

- Policies and procedures
- Training and awareness
- Privacy notices and warning flags
- Confidentiality and end-user agreements
- Access management
- Logging, audit and monitoring
- Privacy breach management
- discipline

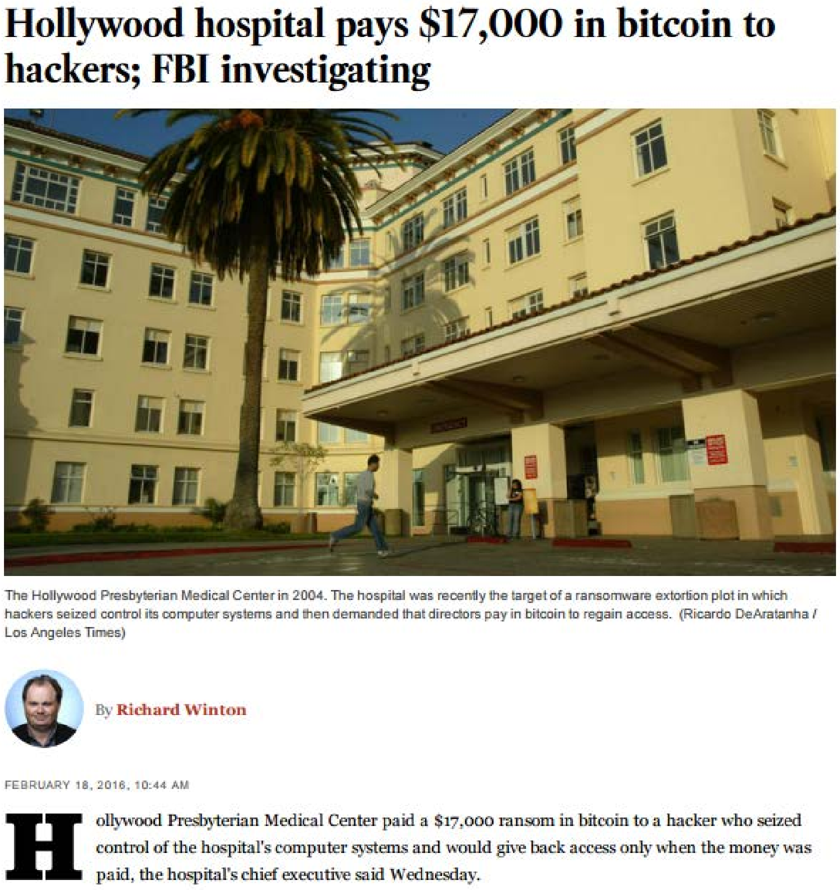
# Agenda

1. Protecting Privacy when Communicating Electronically
2. Communicating PHI by Email
3. Electronic Health Records and Bill 119
4. Mobile Devices
5. Unauthorized Access
6. Ransomware

# 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 data inaccessible until the user pays a ransom to the malware operators to regain access
- Ransom is usually requested in Bitcoin

# Hollywood Presbyterian Medical Center



## Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

The Hollywood Presbyterian Medical Center in 2004. The hospital was recently the target of a ransomware extortion plot in which hackers seized control its computer systems and then demanded that directors pay in bitcoin to regain access. (Ricardo DeAratanha / Los Angeles Times)

By Richard Winton

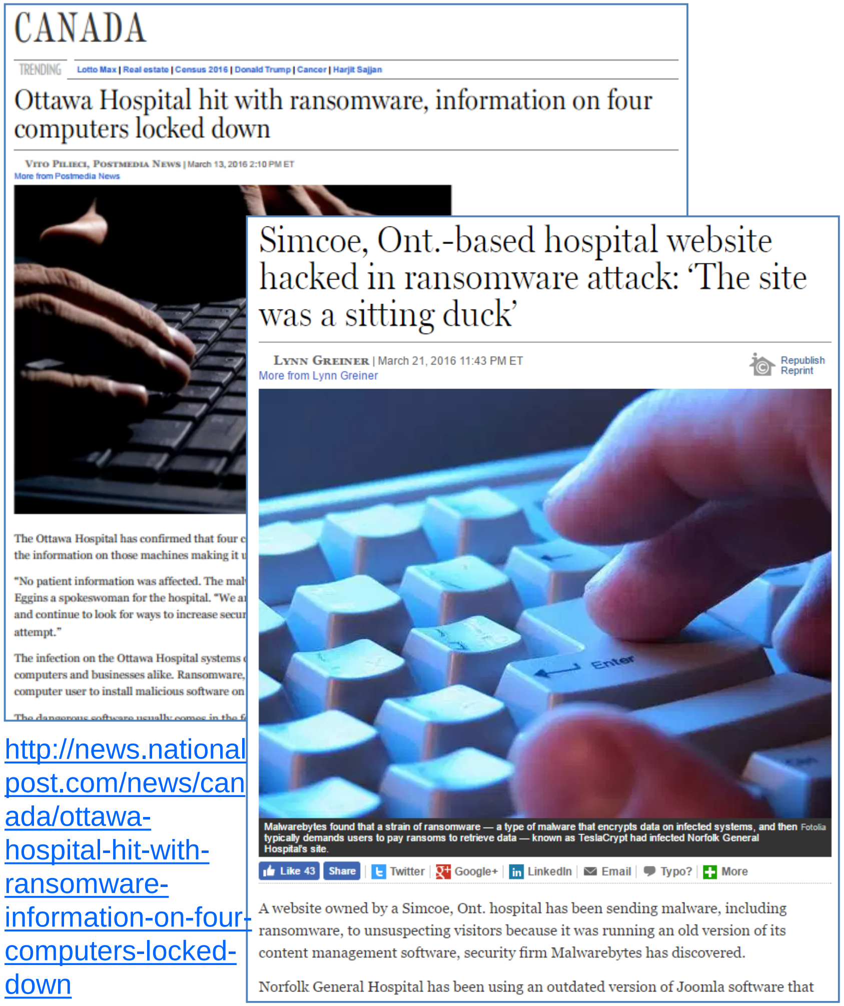
FEBRUARY 18, 2016, 10:44 AM

Hollywood Presbyterian Medical Center paid a $17,000 ransom in bitcoin to a hacker who seized control of the hospital's computer systems and would give back access only when the money was paid, the hospital's chief executive said Wednesday.

http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

- In Feb 2016, hospital was infiltrated by malware that left it without access to digital patient records, some internet-connected medical devices and email for nearly 2 weeks
- The hospital paid a ransom of 40 Bitcoins (about $16,900) to get the decryption key to restore its systems
- Originally demanded >$3 million
- The hospital insisted there was no evidence that the hackers accessed patient records

# The Ottawa Hospital & Norfolk General Hospital



CANADA

TRENDING Lotto Max | Real estate | Census 2016 | Donald Trump | Cancer | Harjit Sajjan

Ottawa Hospital hit with ransomware, information on four computers locked down

Vito Pilieci, Postmedia News | March 13, 2016 2:10 PM ET
More from Postmedia News

The Ottawa Hospital has confirmed that four c
the information on those machines making it u

"No patient information was affected. The mal
Eggins a spokeswoman for the hospital. "We ar
and continue to look for ways to increase secur
attempt."

The infection on the Ottawa Hospital systems
computers and businesses alike. Ransomware,
computer user to install malicious software on

The dangerous software usually comes in the f

Simcoe, Ont.-based hospital website hacked in ransomware attack: 'The site was a sitting duck'

Lynn Greiner | March 21, 2016 11:43 PM ET
More from Lynn Greiner

Republish
Reprint

Malwarebytes found that a strain of ransomware — a type of malware that encrypts data on infected systems, and then typically demands users to pay ransoms to retrieve data — known as TeslaCrypt had infected Norfolk General Hospital's site. Fotolia

A website owned by a Simcoe, Ont. hospital has been sending malware, including ransomware, to unsuspecting visitors because it was running an old version of its content management software, security firm Malwarebytes has discovered.

Norfolk General Hospital has been using an outdated version of Joomla software that

http://news.nationalpost.com/news/canada/ottawa-hospital-hit-with-ransomware-information-on-four-computers-locked-down

- In March 2016, both hospitals were hit with ransomware attacks
- The Ottawa Hospital confirmed four computers were hit, however "no patient information was obtained through the attempt"
- At Norfolk General Hospital the website was hacked and pushed ransomware to computers that visited the website – the hospital restored from back ups

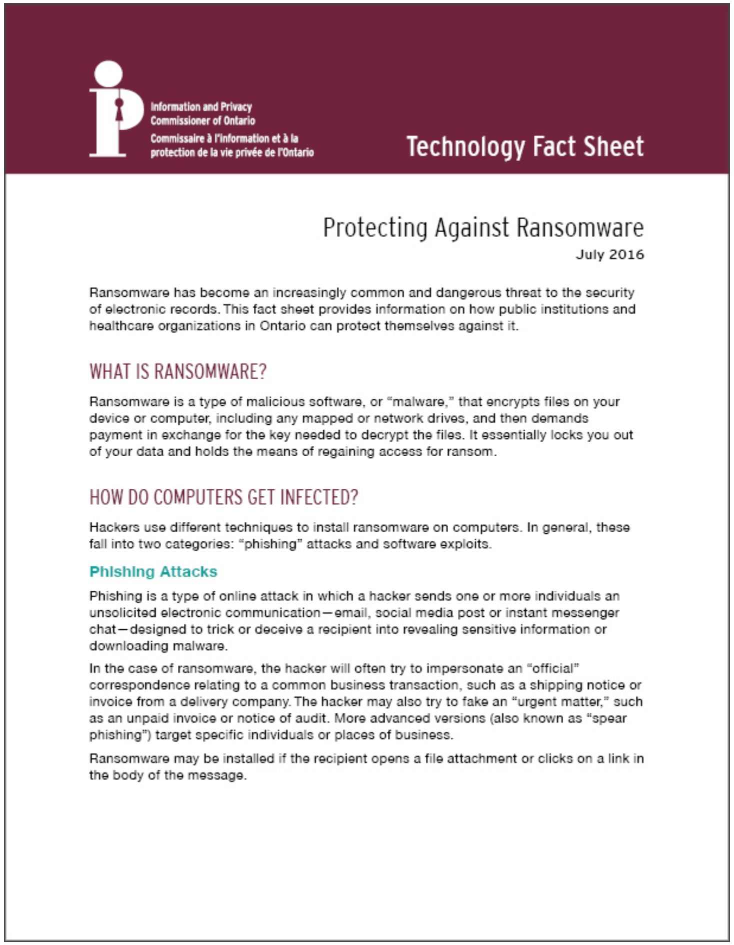
http://business.financialpost.com/fp-tech-desk/cio/simcoe-ont-based-hospital-website-hacked-in-ransomware-attack-the-site-was-a-sitting-duck

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

# 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

# IPC Guidance: Protecting Against Ransomware



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

Technology Fact Sheet

## Protecting Against Ransomware

July 2016

Ransomware has become an increasingly common and dangerous threat to the security of electronic records. This fact sheet provides information on how public institutions and healthcare organizations in Ontario can protect themselves against it.

### WHAT IS RANSOMWARE?

Ransomware is a type of malicious software, or "malware," that encrypts files on your device or computer, including any mapped or network drives, and then demands payment in exchange for the key needed to decrypt the files. It essentially locks you out of your data and holds the means of regaining access for ransom.

### HOW DO COMPUTERS GET INFECTED?

Hackers use different techniques to install ransomware on computers. In general, these fall into two categories: "phishing" attacks and software exploits.

**Phishing Attacks**

Phishing is a type of online attack in which a hacker sends one or more individuals an unsolicited electronic communication—email, social media post or instant messenger chat—designed to trick or deceive a recipient into revealing sensitive information or downloading malware.

In the case of ransomware, the hacker will often try to impersonate an "official" correspondence relating to a common business transaction, such as a shipping notice or invoice from a delivery company. The hacker may also try to fake an "urgent matter," such as an unpaid invoice or notice of audit. More advanced versions (also known as "spear phishing") target specific individuals or places of business.

Ransomware may be installed if the recipient opens a file attachment or clicks on a link in the body of the message.

- What is ransomware?
- How do computers get infected?
  - Phishing attacks
  - Software exploits
- Protecting your organization
- Responding to incidents

# Question?

## Contact us:

2 Bloor Street East, Suite 1400
Toronto, ON
M4W 1A8

**Web:** www.ipc.on.ca

**email:**info@ipc.on.ca

**Telephone:** 416-326-3333 / 1-800-387-0073

**TDD/TTY:** 416-325-7539