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

Update on Strategies and Best Practices for Responding to and Managing Privacy Breaches in Healthcare

April 10, 2017

Sherry Liang

Assistant Commissioner

Information and Privacy Commissioner of Ontario

OSGOODE
OSGOODE HALL LAW SCHOOL
PROFESSIONAL DEVELOPMENT

YORK U
UNIVERSITÉ
UNIVERSITY

Common Causes of Privacy Breaches

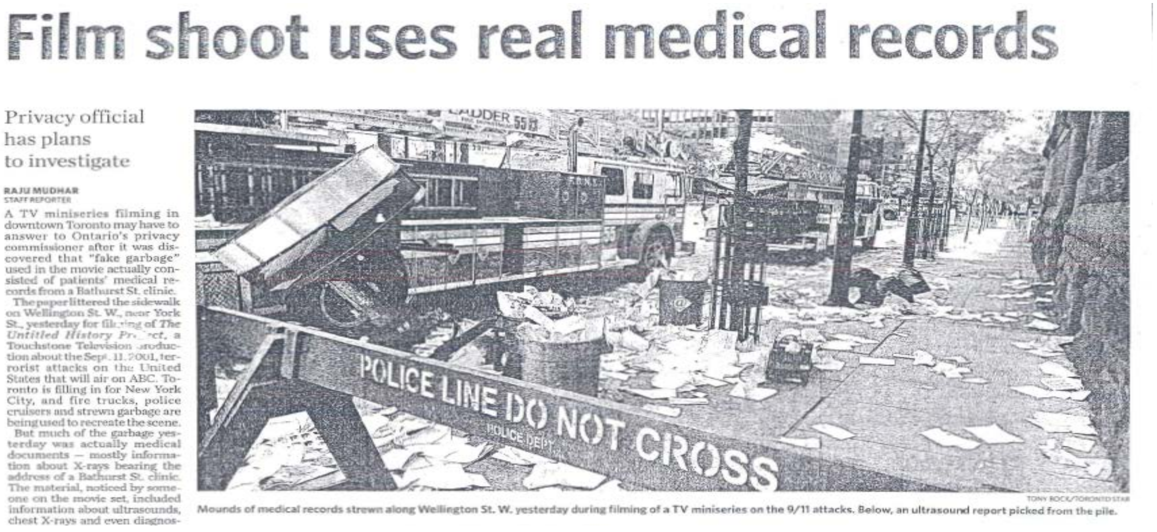
Insecure Disposal of Records

Common Examples

- Records of personal health information in paper format that are intended for shredding, are recycled
- Insecure disposal of records of personal health information in electronic format
- Abandoning records of personal health information when there is a change in practice

Order HO-001
Nature of the Incident

- A medical clinic retained a company to shred records of personal health information dating between 1992 -1994
- Due to a misunderstanding, these records were transported to a recycling company for recycling instead of being shred
- The recycling company sold the records to a special effects company and were used in a film shoot


LADDER 55
POLICE LINE DO NOT CROSS
POLICE DEPT.

Film shoot uses real medical records

Privacy official has plans to investigate

RAJU MUDHAR
STAFF REPORTER

A TV miniseries filming in downtown Toronto may have to answer to Ontario's privacy commissioner after it was discovered that "fake garbage" used in the movie actually consisted of patients' medical records from a Bathurst St. clinic.

The paper littered the sidewalk on Wellington St. W., near York St., yesterday for filming of *The Untitled History Project*, a Touchstone Television production about the Sept. 11, 2001, terrorist attacks on the United States that will air on ABC. Toronto is filling in for New York City, and fire trucks, police cruisers and strewn garbage are being used to recreate the scene.

But much of the garbage yesterday was actually medical documents — mostly information about X-rays bearing the address of a Bathurst St. clinic. The material, noticed by someone on the movie set, included information about ultrasounds, chest X-rays and even diagnos-

TONY BOCK/TORONTO STAR

Mounds of medical records strewn along Wellington St. W. yesterday during filming of a TV miniseries on the 9/11 attacks. Below, an ultrasound report picked from the pile.

Order HO-006
Nature of the Incident

- Records of personal health information were placed in a box designated for recycling as opposed to shredding
- The box designated for recycling was located immediately beside the box designated for shredding
- The records of personal health information were found scattered on the street outside the laboratory in Ottawa

Order HO-003
Nature of the Incident

- A Medical and Rehab Centre closed and left behind records of personal health information
- Landlord asked if the Medical and Rehab Centre wanted to claim property on the premises, but received no response
- Landlord required the immediate removal of the records due to impending renovations

How to Reduce the Risk

- Ensure records of personal health information are thoroughly and securely destroyed
- For paper records – use cross-cut shredding and if particularly sensitive, consider pulverization or incineration
- For electronic records – physically damage and discard the media or if re-use is preferred, using wiping utilities
- Plan for a change in practice:
  - Enter into an agreement identifying the responsibilities of practitioners for the records
  - Arrange for secure retention of the records
  - Notify individuals of a change in practice

Mobile and Portable Devices

Common Examples

- Records of personal health information transferred on unencrypted:
  - Laptops
  - USBs
  - Personal digital assistants (PDAs)
  - Other portable and mobile devices

Orders HO-004, HO-007 and HO-008

- Our office has issued three orders involving personal health information on mobile and portable devices:
  - **Order HO-004 –** Theft of a laptop containing the unencrypted personal health information of 2,900 individuals
  - **Order HO-007 –** Loss of a USB containing the unencrypted personal health information of 83,524 individuals
  - **Order HO-008 –** Theft of a laptop containing the unencrypted personal health information of 20,000 individuals

How to Reduce the Risk….
STOP, THINK, PROTECT

- **STOP** and ask “Do I really need to store personal health information on this device?”
- **THINK** about the alternatives:
    - Would de-identified or coded information serve the purpose?
    - Could the information instead be accessed remotely through a secure connection or virtual private network?
- If you need to retain it on such a device, **PROTECT** it by:
    - Ensuring it is encrypted and protected with strong passwords
    - Retaining the least amount of personal health information
    - Developing policies and procedures, training employees and auditing for compliance

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 …

- 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
- Set out how the individuals can exercise their right of access

Harmonized Privacy Policies and Procedures Needed

Harmonized privacy policies and procedures should address:

- Privacy training
- Logging, auditing and monitoring
- Consent management
- Privacy breach management
- Privacy complaints and inquiries management
- Access and correction
- Governance

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

Orders HO-002, HO-010 and HO-013

- Our office has issued three orders involving unauthorized access to electronic records of personal health information:

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

- An employee accessed records to market and sell RESPs

Detecting and Reducing the Risk of Unauthorized Access

- Clearly explain 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

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 all 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:
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, media reported that the website of Norfolk General Hospital was hacked and ransomware 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

Ransomware:
the Ontario Experience

- In 2016, six ransomware attacks were reported to the IPC by HICs.
- Either individual physicians’ practices or small medical centres.
- Electronic systems were infected with malware that locked the systems.
- Attackers demanded ransoms in exchange for decryption keys to restore access to the data.

Ransomware:
the Ontario Experience

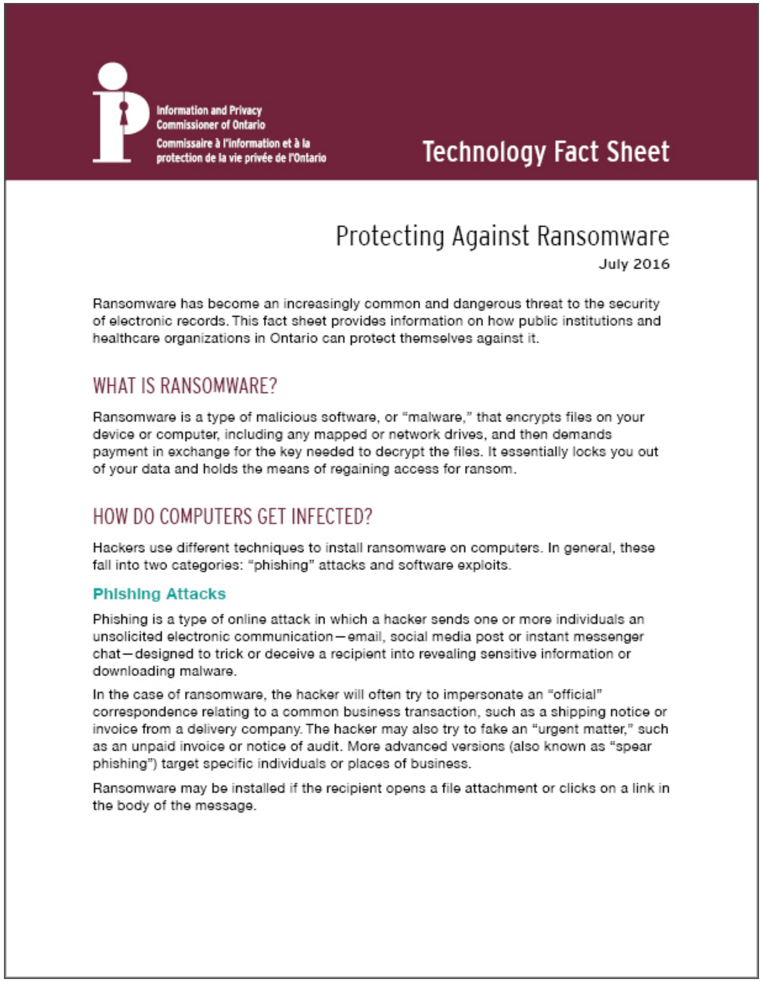
- In two cases the HICs paid the ransom.
  - In one case, decryption key was provided and the data restored.
  - In the other, decryption key was provided but data could not be restored. This HIC was able to restore most of the data from back up files.
- In three cases the ransom was not paid.
  - In two of these the HICs were able to wipe electronic system, reformat server and restore data from a recent back up.
  - In the other case, the HIC lost two years of patient data.

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

Protecting Against Ransomware

- What is ransomware?
- How do computers get infected?
  - Phishing attacks
  - Software exploits
- Protecting your organization
- Responding to incidents
- Available at www.ipc.on.ca



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.

Potential Consequences of Privacy Breaches

Potential Consequences to Patients

If inadequate attention is paid to privacy, this may result in:

- Discrimination, stigmatization and psychological or economic harm to patients based on the information
- Patients being deterred from seeking testing or treatment
- Patients may withhold or falsify the information provided to their health care providers
- Loss of trust or confidence in the health system

Potential Consequences to Health Care Providers

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

Offences

- *PHIPA* creates offences for contravention, including wilfully collecting, using or disclosing personal health information in contravention of the statute
- Anyone can commence a prosecution for offences under *PHIPA*, with Attorney General's consent
- On conviction, an individual may be liable for a fine of up to $100,000 and a corporation up to $500,000

Statutory or Common Law Actions

- Action based on *PHIPA* contravention: Can sue for actual harm suffered if Commissioner has made final order or offence results in final conviction
  - If the conduct was willful or reckless, court may award up to $10,000 for mental anguish
- Action based on general law: In 2012, the Ontario Court of Appeal recognized a common law cause of action in tort for invasion of privacy

Common Law Action –
Tort of “Intrusion Upon Seclusion”

- In *Jones* v. *Tsige*, the Ontario Court of Appeal recognized a new common law action for “intrusion upon seclusion”
- There are three required elements of the cause of action:
  - Intentional or reckless conduct by the defendant
  - The defendant must have invaded, without lawful justification, the plaintiff’s private affairs or concerns
  - A reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish
- Damages will ordinarily be measured by a modest conventional sum – generally to a maximum of $20,000

Tort of Intrusion Upon Seclusion in the Health Context – *Hopkins v. Kay*

- Does the new tort apply to health privacy, given availability of *PHIPA* remedies?
- Action started against Peterborough Regional Health Centre alleging breach of privacy of about 280 patients
- The Hospital argued *PHIPA* was an "an exhaustive code" and common law claim for invasion of privacy does not apply to patient records
- Our office intervened and took the position that *PHIPA* can co-exist with common law claims for invasion of privacy

Hopkins v. Kay

- **In February 2015,** the Court of Appeal agreed, stating that *PHIPA* expressly contemplates other proceedings in relation to personal health information.
- In **October 2015,** an application for leave to appeal was dismissed by the Supreme Court of Canada.

Referrals to Prosecution

- During investigation of breaches, IPC may refer the case to the Attorney General for prosecution
- In deciding whether or not to refer a case, some of the factors the IPC considers are:
  - Were the actions "willful"
    - recent privacy training
    - recently signed confidentiality agreement
    - ignoring privacy warnings on the system
  - Number of occurrences
  - Additional use or disclosure of the information
  - Motive
  - Disciplinary action taken; complaint to professional college
  - Interests/views of the patient

Referrals for Prosecution

2011 – A nurse at North Bay Health Centre

2015 – Two radiation therapists at University Health Network

2015 – A social worker at a family health team

2015 – A registration clerk at a regional hospital

2016 – A regulated professional at a Toronto hospital

Outcome of Referrals

- Case from 2011 dismissed for delay
- UHN case
  - Pled guilty; each individual fined $2000
- Registration clerk
  - 443 patients
  - Pled guilty; $10,000 fine, $2500 victim surcharge
- Member of Family Health Team in small community
  - Pled guilty; $20,000 fine, $5000 victim surcharge
- Health professional at hospital
  - Referred to AG in 2016; no word on charges

What to do in the Event of a Privacy Breach

Implementation, Identification and Containment

- Determine whether a privacy breach has occurred
- Identify the personal health information compromised
- Notify senior management of the privacy breach
- Implement containment measures to ensure personal health information is protected from further theft, loss or unauthorized use or disclosure, for example:
  - Ensure no copies of the records have been made
  - Ensure the records are either retrieved or securely destroyed
  - Obtain confirmation that the records have been securely destroyed

Notification

- *PHIPA* requires individuals to be notified at the first reasonable opportunity if their personal health information is stolen, lost or accessed by unauthorized persons
- Consider best means of notifying – if in doubt, consult with IPC
- The notification should at minimum advise individuals of:
  - Details of the breach
  - The type of personal health information in issue
  - Steps taken to address the privacy breach, immediate and long term
  - HIC Contact information
  - IPC contact information in the event they wish to file a complaint

Investigation and Remediation

- Conduct an investigation in order to:
  - Determine whether the breach has been effectively contained
  - Ensure notification has been provided to affected individuals
  - Review the circumstances surrounding the privacy breach
  - Review the adequacy of existing policies and procedures
  - Develop recommendations to prevent similar future breaches
- Document the investigation and recommendations
- Implement the recommendations to prevent similar breaches in the future
- Work with IPC on any additional investigation or action

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
www.ipc.on.ca
info@ipc.on.ca