

PROTECTING PRIVACY WHEN USING NEW...AND NOT SO NEW TECHNOLOGIES

PHIPA Summit
- December 4, 2015 -

Debra Grant, Director of Health Policy

Manuela Di Re, Director of Legal Services

Why is the Protection of Privacy So Critical?

The need to protect the privacy of individuals' personal health information has never been greater given the:

- Extreme sensitivity of personal health information
- Greater 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

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

- 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

Relevant Statutory Provisions

Security of Personal Health Information

- The *Personal Health Information Protection Act, 2004* (“the Act”) requires records of personal health information to be retained, transferred and disposed of in a secure manner
- The Act also requires steps that are reasonable in the circumstances be taken to ensure that:
 - Personal health information is protected against theft, loss and unauthorized use or disclosure
 - Records of personal health information are protected against unauthorized copying, modification and disposal

Data Minimization

- The *Act* also provides that a health information custodian must not collect, use or disclose:
 - Personal health information if other information will serve the purpose of the collection, use or disclosure; and
 - More personal health information than is reasonably necessary to meet the purpose of the collection, use or disclosure.

Privacy Protection and Various Technologies





1. Fax



Best Practices for Transferring Personal Health Information by Fax

- Develop policies and procedures for transferring personal health information by fax that, among other things:
 - Require fax machines to be located in secure locations that are not generally accessible to the public
 - Require confirmation of the telephone number prior to dialling, including regular checks of master lists and programmed numbers
 - Set out the steps required to ensure that the telephone number of the recipient corresponds to the telephone number dialled
 - Require the sender to confirm the success of a fax transmission
 - Set out the procedure to be followed when you are notified that a fax was received by a recipient in error

Best Practices for Transferring Personal Health Information by Fax

- Set out the procedure to be followed when you receive a fax in error, including notification of the sender and obtaining confirmation as to whether it should be returned to the sender or securely destroyed
- Require the use of standard cover sheets containing:
 - ✓ The name, title and organization of the sender and recipient
 - ✓ The total number of pages faxed
 - ✓ A box that allows you to “check off” whether the recipient should confirm receipt
 - ✓ A notice that the information is confidential and subject to the *Act*
 - ✓ Instructions for the recipient to follow if the fax is received in error
- Develop policies and procedures for securely disposing of fax machines that store personal health information



2. Email



Challenges Posed by Email

- Email may be vulnerable to interception and hacking by unauthorized third parties
- Email may be used to transmit malicious code
- Email may be forwarded or modified without the consent of the sender
- Email may be inadvertently transmitted to the wrong recipient
- Email may be accessed on portable devices which are vulnerable to loss and theft



Best Practices for Transmitting Personal Health Information by Email

- When communicating personal health information among health information custodians use a secure email solution such as the ONE mail service offered by eHealth Ontario
- Whenever possible, when communicating with any other individuals, use secure messaging like that offered through a patient portal or other secure messaging application
- In circumstances where it is not practical to use secure email or other more secure means to communicate with individuals, implement the additional privacy and security measures outlined in the following slides

Best Practices for Transmitting Personal Health Information by Email

- Develop policies and procedures setting out when, how and the purposes for which personal health information may be sent and/or received by secure and unsecure email
- Implement physical, technical and administrative safeguards to protect personal health information sent and/or received by secure and unsecure email
- Minimize the collection, use and disclosure of personal health information sent and/or received by secure and unsecure email
- Provide notice before sending and/or receiving personal health information by secure and unsecure email
- Provide privacy and security training for sending and receiving personal health information by secure and unsecure email

Best Practices for Transmitting Personal Health Information by Unsecure Email

- In addition to following the best practices noted in the previous slides, before sending and/or receiving personal health information by email that may not be secure:
 - Ensure that individuals understand and accept the risk of unauthorized collection, use and disclosure of their personal health information
 - Obtain express consent for sending and/or receiving personal health information by email that may not be secure
- *Stay tuned for new email guidance from our office*

3. Mobile and Portable 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

Best Practices for Retaining Personal Health Information on Mobile or Portable Devices

- Avoid retaining personal health information on such devices unless it is necessary for the purpose
- Consider alternatives to retaining personal health information on such devices, such as retaining:
 - De-identified information on the device,
 - Encoded information on the device and storing the code to unlock identifying information separately on a secure computing device, or
 - Personal health information on a secure server and accessing it remotely through a secure connection or virtual private network

Best Practices for Retaining Personal Health Information on Mobile or Portable Devices

- If it is necessary to retain personal health information:
 - 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 to ensure they continue to be effective in minimizing privacy risks

What is Strong Encryption?

- Strong encryption also includes ensuring that:
 - The encryption solution has been successfully deployed
 - The encryption solution continues to function appropriately
 - Error messages indicating a malfunction of the encryption solution are monitored and responded to immediately
 - Encryption keys of a sufficient length are used
 - Safeguards are implemented to protect encryption keys from theft, loss and access by unauthorized persons
 - The encryption solution is subject to ongoing security reviews and updates

What Are Strong Passwords?

- Strong passwords consist of at least eight characters
- Strong passwords combine letters, numbers and symbols in what appear to be a random string
- Strong password protection includes the development and implementation of policies and procedures:
 - Identifying the minimum and maximum password length
 - Outlining the standard for password composition
 - Providing for automatic expiry after a defined period
 - Requiring the device be locked after a defined number of failed log-in attempts
 - Imposing a mandatory system-wide password-protected screen saver after a pre-defined period of inactivity
 - Requiring agents to keep passwords private



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, train and audit compliance

Guidelines and Best Practices on Mobile and Portable Devices

- Our office has issued numerous guidelines and best practices on mobile and portable devices, such as:
- *Encrypting Personal Health Information on Mobile Devices*
 - *Health-Care Requirement for Strong Encryption*
 - *Wireless Communication Technologies: Safeguarding Privacy and Security*
 - *Safeguarding Privacy In a Mobile Workplace*
 - *Innovative Wireless Home Care Services: Protecting Privacy and Personal Health Information*



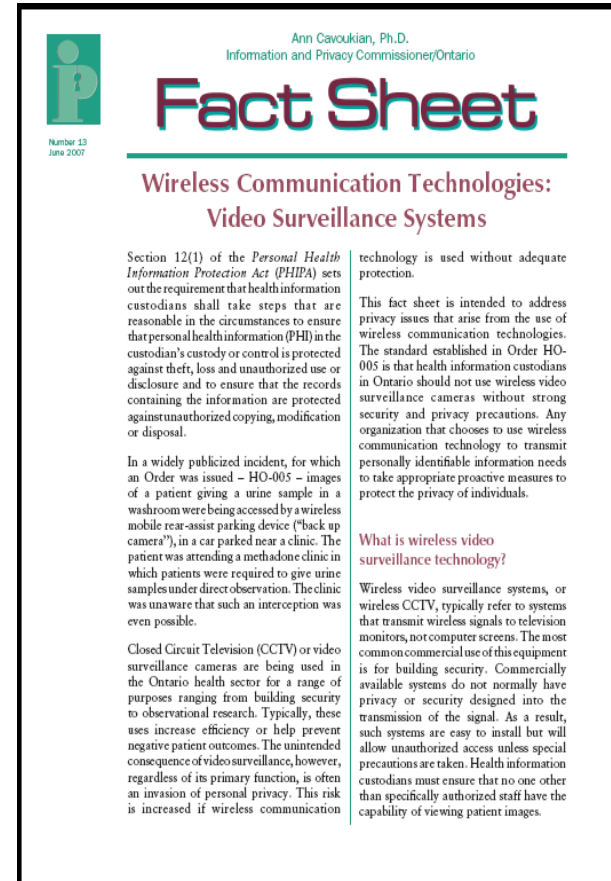
4. Wireless

Order HO-005

- Received a report that a wireless mobile rear-assist parking device captured the video image of an individual providing a urine sample in the washroom of a methadone clinic
- The methadone clinic installed a wireless surveillance camera to monitor individuals providing urine samples
- Images were not recorded, images were only monitored in real time by a nurse working at the methadone clinic
- The signal from the surveillance camera was not encrypted
- Consent was obtained for the use of the surveillance camera

Best Practices When Using Wireless Communication Technologies

- Wireless communication technologies should not be used to transmit personal health information without strong security and privacy precautions
- Health information custodians should:
 - Conduct privacy impact assessments and annual security and privacy audits
 - Ensure privacy and security requirements are explicit in the procurement process
 - Ensure the vendor selection process requires signal protection to prevent unauthorized access to personal health information, through an encrypted or scrambled signal



Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

Fact Sheet

Number 13
June 2007

Wireless Communication Technologies: Video Surveillance Systems

Section 12(1) of the *Personal Health Information Protection Act (PHIPA)* sets out the requirement that health information custodians shall take steps that are reasonable in the circumstances to ensure that personal health information (PHI) in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

In a widely publicized incident, for which an Order was issued – HO-005 – images of a patient giving a urine sample in a washroom were being accessed by a wireless mobile rear-assist parking device (“back up camera”), in a car parked near a clinic. The patient was attending a methadone clinic in which patients were required to give urine samples under direct observation. The clinic was unaware that such an interception was even possible.

Closed Circuit Television (CCTV) or video surveillance cameras are being used in the Ontario health sector for a range of purposes ranging from building security to observational research. Typically, these uses increase efficiency or help prevent negative patient outcomes. The unintended consequence of video surveillance, however, regardless of its primary function, is often an invasion of personal privacy. This risk is increased if wireless communication technology is used without adequate protection.

This fact sheet is intended to address privacy issues that arise from the use of wireless communication technologies. The standard established in Order HO-005 is that health information custodians in Ontario should not use wireless video surveillance cameras without strong security and privacy precautions. Any organization that chooses to use wireless communication technology to transmit personally identifiable information needs to take appropriate proactive measures to protect the privacy of individuals.

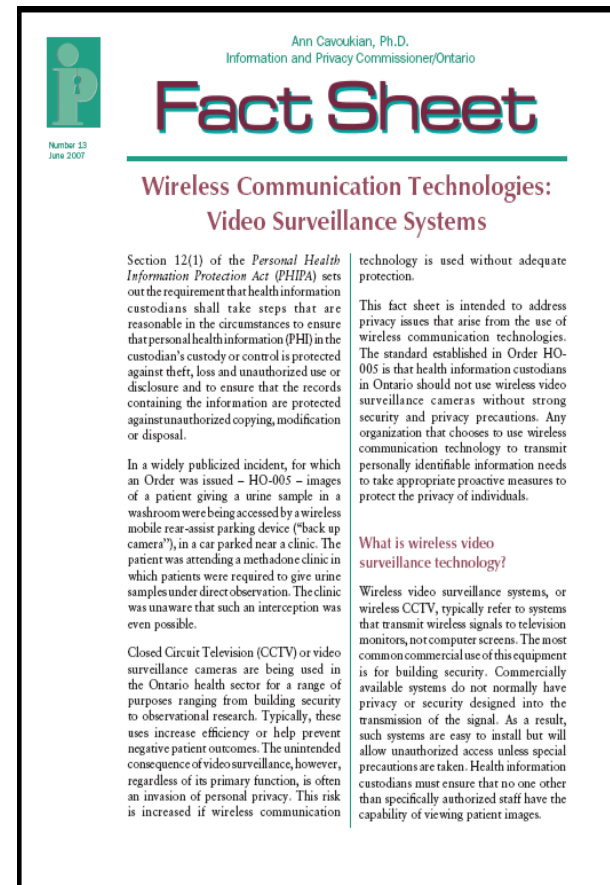
What is wireless video surveillance technology?

Wireless video surveillance systems, or wireless CCTV, typically refer to systems that transmit wireless signals to television monitors, not computer screens. The most common commercial use of this equipment is for building security. Commercially available systems do not normally have privacy or security designed into the transmission of the signal. As a result, such systems are easy to install but will allow unauthorized access unless special precautions are taken. Health information custodians must ensure that no one other than specifically authorized staff have the capability of viewing patient images.



Best Practices When Using Wireless Communication Technologies

- Ensure the signal cannot be intercepted by unauthorized persons
- Ensure the wireless communication technology is off except when used for designated purposes
- If using such technologies to conduct surveillance, ensure you follow our office's *Guidelines for the Use of Video Surveillance Cameras*
- Ensure agents receive special technical training on the privacy and security issues associated with wireless communication technologies



Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

Fact Sheet

Number 13
June 2007

Wireless Communication Technologies: Video Surveillance Systems

Section 12(1) of the *Personal Health Information Protection Act (PHIPA)* sets out the requirement that health information custodians shall take steps that are reasonable in the circumstances to ensure that personal health information (PHI) in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

In a widely publicized incident, for which an Order was issued – HO-005 – images of a patient giving a urine sample in a washroom were being accessed by a wireless mobile rear-assist parking device (“back up camera”), in a car parked near a clinic. The patient was attending a methadone clinic in which patients were required to give urine samples under direct observation. The clinic was unaware that such an interception was even possible.

Closed Circuit Television (CCTV) or video surveillance cameras are being used in the Ontario health sector for a range of purposes ranging from building security to observational research. Typically, these uses increase efficiency or help prevent negative patient outcomes. The unintended consequence of video surveillance, however, regardless of its primary function, is often an invasion of personal privacy. This risk is increased if wireless communication technology is used without adequate protection.

This fact sheet is intended to address privacy issues that arise from the use of wireless communication technologies. The standard established in Order HO-005 is that health information custodians in Ontario should not use wireless video surveillance cameras without strong security and privacy precautions. Any organization that chooses to use wireless communication technology to transmit personally identifiable information needs to take appropriate proactive measures to protect the privacy of individuals.

What is wireless video surveillance technology?

Wireless video surveillance systems, or wireless CCTV, typically refer to systems that transmit wireless signals to television monitors, not computer screens. The most common commercial use of this equipment is for building security. Commercially available systems do not normally have privacy or security designed into the transmission of the signal. As a result, such systems are easy to install but will allow unauthorized access unless special precautions are taken. Health information custodians must ensure that no one other than specifically authorized staff have the capability of viewing patient images.



Information and Privacy
Commissioner of Ontario

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

4. Electronic Medical Records

Addressing Privacy In The Transition to Electronic Medical Records

Personal health information may be vulnerable when transitioning from paper to electronic medical records because:

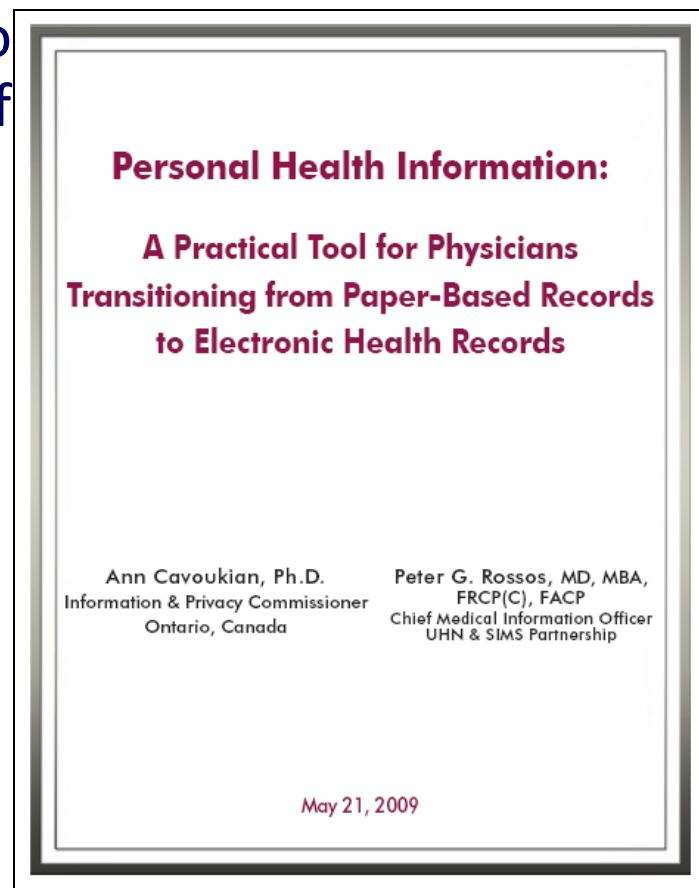
- Staff may not be trained on the electronic medical record system
- The electronic medical record system may not be fully functional
- Privacy and security features may be turned off or set to minimal protection by default
- Conversion from paper to electronic format may require frequent access to the records by larger numbers of individuals, including third parties, during the conversion process
- Records may be duplicated in paper and electronic format



A Practical Tool for Physicians

Transitioning to Electronic Medical Records

- Our office jointly published a toolkit to manage privacy issues with a Chief Medical Information Officer
- The toolkit addresses measures such as:
 - Educating and training staff
 - Implementing access controls
 - Implementing strong passwords
 - Auditing access to electronic records
 - Managing the retention, transfer and disposal of paper records
 - Drafting/updating policies and procedures



5. Shared Electronic Health Record 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 challenges for compliance with the *Act*

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
- Ensure all health information custodians are operating under common privacy standards
- Set out how the rights of individuals will be exercised

Harmonized Privacy Policies and Procedures Needed

Harmonized privacy policies and procedures should address:

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



Unauthorized Access to Electronic Records



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

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

Examples from Other Jurisdictions—Alberta

Prosecution in 2007

- A medical office clerk plead guilty and was fined \$10,000 under the *Health Information Act*
- Accessed the information of the wife of a man with whom she was having an affair using Alberta Netcare and fax
- Accessed the information on six different occasions

Investigation Report H2011-IR-004

- Physician used Alberta Netcare to view records of a partner's former spouse and mother and girlfriend of the former spouse
- Used the accounts of colleagues who failed to log out
- Viewed records on 21 occasions over a period of 15 months

Examples from Other Jurisdictions—Alberta

Investigation Report Pending

- Pharmacist plead guilty and was fined \$15,000 under the *Health Information Act*
- Used Alberta Netcare to view the records of a number of women who attended her church and posted the prescription information of some of the women on Facebook

Prosecution in 2014

- A medical laboratory assistant received a four month conditional sentence, eight months probation and a \$500 fine
- Accessed the personal health information of 34 individuals and uttered forged documents under the *Criminal Code*

Examples from Other Jurisdictions— Saskatchewan

Investigation Report H-2010-001

- Pharmacist used the Pharmaceutical Information Program, a domain repository in Saskatchewan's electronic health record, to view drug profiles of three individuals on nine occasions after a business arrangement with the individuals dissolved

Investigation Report H-2013-001

- Employees of Regina Qu'Appelle Regional Health Authority viewed their own health information, viewed and modified the health information of other employees and viewed the health information of other individuals

How to Reduce the Risk...

- 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

New Guidance Document: Detecting and Deterring Unauthorized Access



Detecting and Deterring
Unauthorized Access to
Personal Health Information

- 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

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

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca