

# **CURRENT TRENDS AND KEY ISSUES UNDER THE *PERSONAL HEALTH INFORMATION PROTECTION ACT, 2004***

**OSMT Connect – Newmarket  
November 4, 2017**

**Brendan Gray, Health Law Counsel  
Office of the Information and Privacy Commissioner of Ontario (IPC)**

# DISCLAIMER

THIS PRESENTATION IS:

- PROVIDED FOR INFORMATIONAL PURPOSES,
- NOT LEGAL ADVICE, AND
- NOT BINDING ON THE IPC.

# Outline

- The *Personal Health Information Protection Act* (the *Act* or *PHIPA*)
  - Quick overview of the application of the *Act*
  - What's New
  - Bill 119
  - Interaction of *FIPPA/MFIPPA* and *PHIPA*
  - Detecting and Deterring Unauthorized Access
  - Discipline by Regulatory Colleges

# 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” 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 personal health information by non-health information custodians that receive personal health information from health information 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, including information that consists of the health history of the individual's family
- Relates to the provision of health care to the individual, including the identification of a person as a provider of health care to the individual
- 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 centre, program or service for community health or mental health whose primary purpose is the provision of 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
- Every local health integration network



Information and Privacy  
Commissioner of Ontario

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

# Definition of Agent

- An agent is a person that, with the authorization of a health information custodian, acts for or on behalf of the custodian in respect of personal health information
  
- It is irrelevant whether or not the agent:
  - is employed by the health information custodian
  - is remunerated by the health information custodian
  - has the authority to bind the health information custodian
  
- A health information custodian remains responsible for personal health information 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 health information custodians and their agents under the *Act*
- These duties generally fall into four categories:
  - Collection, use and disclosure of personal health information
  - Security of personal health information
  - Responding to requests for access to and correction of records of personal health information
  - Transparency of information practices

# **COLLECTION, USE AND DISCLOSURE AND CONSENT**



# General Provisions Related to Collection, Use and Disclosure

- Not permitted to collect, use or disclose personal health information if other information will serve the purpose
- Not permitted to collect, use or disclose more personal health information than reasonably necessary
- Not permitted to collect, use or disclose personal health information UNLESS:
  - The individual consents, or
  - The collection, use or disclosure is permitted or required by the Act to be made without consent

# Elements for Valid Consent

Consent, whether express or implied, must:

1. Be the consent of the individual or his or her substitute decision-maker (where applicable),
2. Be knowledgeable, meaning, it must be reasonable to believe that the individual knows:
  - The purpose of the collection, use or disclosure; and
  - That the individual may give or withhold consent
3. Relate to the information, and
4. Not be obtained by deception or coercion.

# Notice of Purposes

- A custodian may rely on a *Notice of Purposes* to support the reasonable belief that an individual knows the purpose of the collection, use or disclosure of personal health information unless it is not reasonable
- A *Notice of Purposes*:
  - Must be posted where it is likely to come to the attention of the individual or must be provided to the individual;
  - Must outline the purposes for which the custodian collects, uses or discloses personal health information; and
  - Should advise the individual that he or she has the right to give or withhold consent
- A *Notice of Purposes* is not required when consent may be assumed to be implied but it is a best practice

# Types of Consent

- There are three types of consent under the *Act*:
  - Express consent
  - Implied consent
  - Assumed implied consent
- Assumed implied consent provisions are sometimes referred to as the “circle of care” provisions

# Express Consent

- Consent may be express or implied, except when the Act specifies that consent must be express
- Express consent is not a defined term in the *Act*
- It is commonly understood as consent that has been clearly and unmistakably given orally or in writing
- In general, express consent is required to:
  - Disclose personal health information to a non-health information custodian
  - Disclose personal health information to another health information custodian for a purpose other than the provision of health care
  - Collect, use or disclose personal health information for marketing
  - Collect, use or disclose personal health information for fundraising (if it amounts to more than the name and address of the individual)

# Implied Consent

- In all other circumstances, consent may be implied
- Implied consent is not a defined term in the *Act*
- Commonly understood as a consent that one concludes has been given based on an individual's action or inaction in particular factual circumstances
- For example, consent may be implied:
  - To *collect* or *use* personal health information for any purpose, subject to certain exceptions
  - To *disclose* personal health information to another health information custodian for the provision of health care

# Assumed Implied Consent

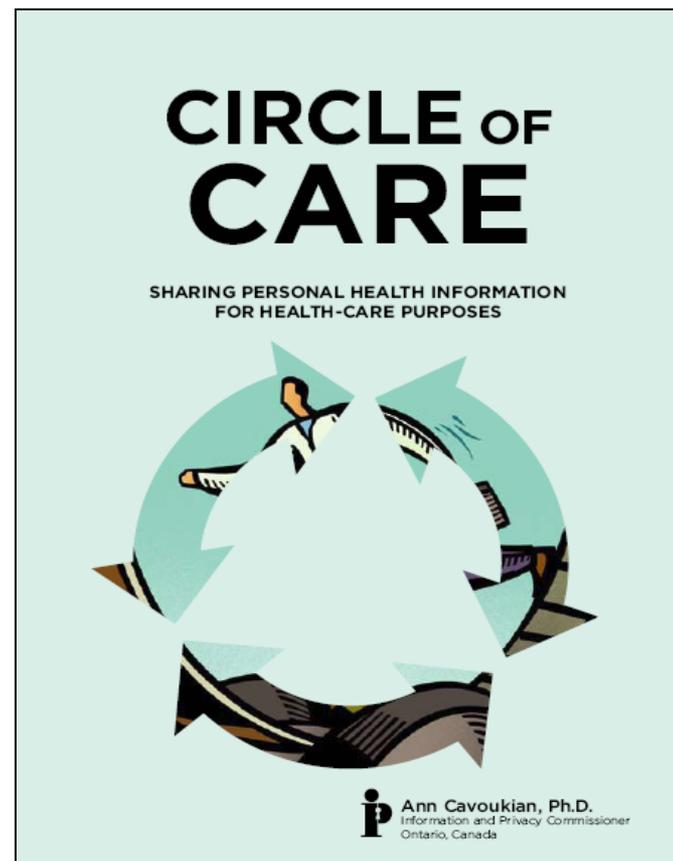
- Sometimes referred to as “Circle of Care”
- Section 20(2) of the Act provides:
  - (2) A health information custodian described in paragraph 1, 2, 3 or 4 of the definition of “health information custodian” in subsection 3 (1), that receives personal health information about an individual from the individual, the individual’s substitute decision-maker or another health information custodian for the purpose of providing health care or assisting in the provision of health care to the individual, is entitled to assume that it has the individual’s implied consent to collect, use or disclose the information for the purposes of providing health care or assisting in providing health care to the individual, unless the custodian that receives the information is aware that the individual has expressly withheld or withdrawn the consent.
- In the context of a disclosure, the disclosure must be made to another health information custodian

# Circle of Care: Sharing Personal Health Information for Health Care Purposes

The guide was published to clarify the circumstances in which consent may be *assumed* to be implied by custodians

Members of the working group who participated in publishing the guide, included:

- Information and Privacy Commissioner/ Ontario
- College of Physicians and Surgeons of Ontario
- Ontario Association of Community Care Access Centres
- Ontario Association of Non-Profit Homes and Services for Seniors
- Ontario Long Term Care Association
- Ontario Hospital Association
- Ontario Medical Association
- Ontario Ministry of Health and Long-Term Care



# Withholding and Withdrawing Consent and Express Instructions

- The *Act* provides individuals with the right, subject to certain exceptions, to expressly:
  - Withhold or withdraw consent to the collection, use or disclosure of personal health information, including for the purpose of providing health care; and
  - Instruct that their personal health information not be used or disclosed without consent for health care purposes as set out in sections 37(1)(a), 38(1)(a) and 50(1)(e) of the Act
- These are referred to as the “lock-box” provisions, although lock-box is not a term found in the Act

# Duties Arising From Withholding and Withdrawing Consent or Express Instructions

1. A custodian must comply with the decision to withhold or withdraw consent or to provide an express instruction unless:
  - The individual changes his or her mind,
  - The Act permits the collection, use or disclosure to be made without consent, except as set out in sections 37(1)(a), 38(1)(a) and 50(1)(e)
2. Compliance may be achieved through policies, procedures or manual processes and/or electronic or technological means
3. Where a custodian is prevented from disclosing personal health information to certain other custodians that is believed to be reasonably necessary for the provision of health care:
  - The disclosing health information custodian **must** notify the other health information custodian of that fact; and
  - The receiving health information custodian may explore the matter with the individual and seek consent to access the locked information

# Collections, Uses and Disclosures Permitted Without Consent

- Collections of personal health information permitted without consent are set out in section 36 of the *Act*
- Uses of personal health information permitted without consent are set out in section 37 of the *Act*
- Disclosures permitted without consent are set out in sections 38 – 48 and section 50 of the *Act*
  - Example: Under *PHIPA*, health information custodians may disclose personal health information as permitted or required under other Acts, subject to any prescribed requirements or restrictions. A regulation to the *Laboratory and Specimen Collection Centre Licensing Act*, requires disclosure of reportable diseases to a medical officer of health or health unit. *PHIPA* permits this disclosure as no requirements or restrictions are prescribed.

# REQUESTS FOR ACCESS AND CORRECTION



# Right of Access to Records of Personal Health Information

- Individuals have a right of access to their records of personal health information subject to exclusions and exceptions
- A health information custodian must respond to a request for access within 30 days, subject to a possible 30 day extension
- When granting access, health information custodians must:
  - Make the record of personal health information available for examination and, upon request, provide a copy to the individual
  - Take reasonable steps to be satisfied as to identity
  - Provide an explanation of any term, code or abbreviation used in the records of personal health information if reasonably practical
- A fee may be charged for access provided an estimate is first provided and the fee does not exceed reasonable cost recovery (see IPC Orders HO-009 and HO-014)

# Access to Records of Personal Health Information, cont'd

- Requests for access should be in writing and must provide enough information to allow the custodian to identify and locate the record
- Nothing in the *Act* prevents a custodian from granting access to a record in response to an oral request
- Nothing in the *Act* prevents a custodian from communicating with an individual about his or her record of personal health information



# Requests for Correction of a Record of Personal Health Information

- Individuals may request correction of their record of personal health information if they believe it is inaccurate or incomplete
- A health information custodian must respond to a request for correction within 30 days following receipt
- A health information custodian must correct the record of personal health information if the individual demonstrates that the record is incomplete or inaccurate unless:
  - It consists of a record that was not originally created by the health information custodian and the health information custodian has insufficient expertise, knowledge or authority to correct the record; or
  - It consists of professional opinion or observation that the health information custodian has made in good faith

# WHAT'S NEW

# Recent Prosecution Under PHIPA

- March 2015, the IPC was notified that a Masters of Social Work student on educational placement illegally accessed health records of family, friends, and other individuals
- After investigating, IPC referred matter to the Attorney General
- In her plea, student admitted to unlawfully accessing PHI of 139 people between September 9, 2014, and March 5, 2015

# Recent Prosecution Under PHIPA (Cont'd)

- Ordered to pay:
  - \$20,000 fine
  - \$5,000 victim surcharge
- Highest fine to date for a health privacy breach in Canada
- HICs are obligated to ensure safeguards in place to prevent unlawful access



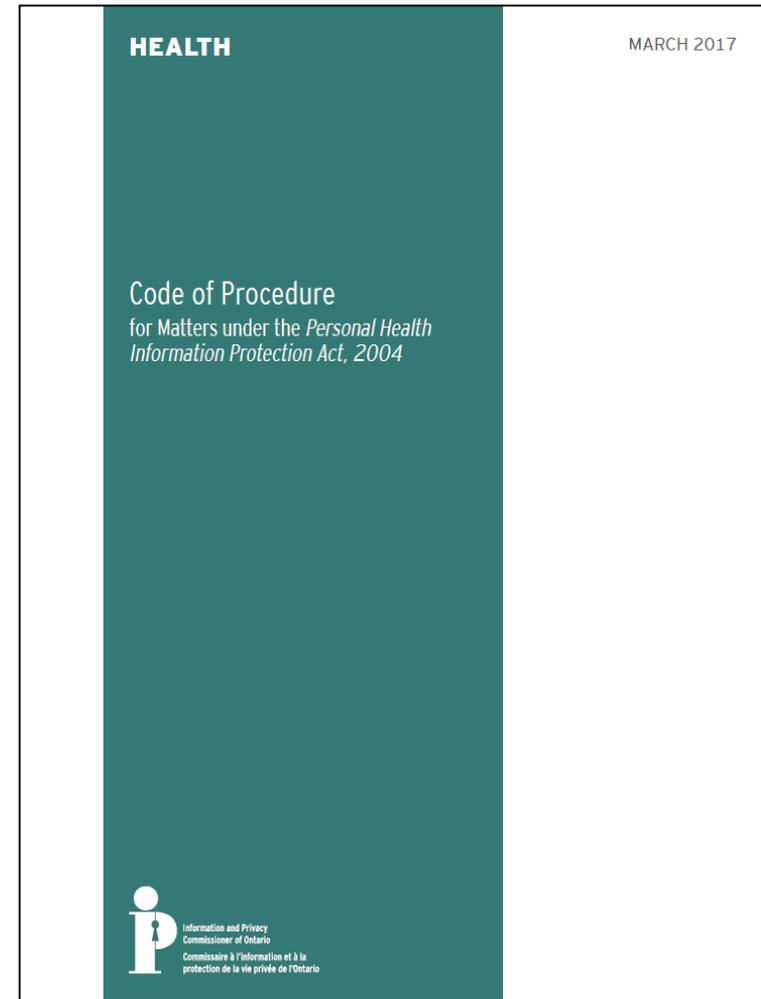
# Recent Prosecution Under PHIPA (Cont'd)

- *“The various victims have provided victim impact statements which are quite telling in terms of the sense of violation, the loss of trust, the loss of faith in their own health care community, and the utter disrespect [the accused] displayed towards these individuals.”*
- *“I have to take [the effect of deterrence on the accused] into consideration, but realistically, it’s general deterrence, and that has to deal with every other health care professional or someone who is governed by this piece of legislation. This is an important piece of legislation ...”*

– Justice of the Peace, Anna Hampson

# New *PHIPA* Code of Procedure

- New code arising from internal review
- Effective March 15, 2017, applies to all IPC files under *PHIPA*
- Now a single code applicable to all matters arising under *PHIPA*
- New practice directions provide guidance to parties exercising their rights and complying with their obligations under the new code



# 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.

# Communicating PHI by Email – *Cont'd*

- For emailing PHI between custodians, IPC expects encryption, barring exceptional circumstances
- For emailing PHI between custodians and patients
  - use encryption where feasible
  - where encryption is not feasible, only communicate PHI through unencrypted email where reasonable using risk-based approach
  - approach to emailing patients should be captured in a written policy
  - notify patients of email policy and obtain consent prior to use of unencrypted email

# 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

# **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

# 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
- 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
- The Commissioner must also be notified if the circumstances surrounding the theft, loss or unauthorized collection, use or disclosure meets certain prescribed requirements



# Breach Notification, cont'd

- Regulations prescribing when the Commissioner must be notified of a theft, loss or unauthorized use or disclosure came into force October 1, 2017
- The IPC recently published a guidance document explaining when we expect that a privacy breach will be reported to the Commissioner.

SEPTEMBER 2017

## Reporting a Privacy Breach to the Commissioner

GUIDELINES FOR THE HEALTH SECTOR

To strengthen the privacy protection of personal health information, the Ontario government has amended the *Personal Health Information Protection Act* (the act). Under section 12(3) of the act and its related regulation, custodians must notify the Information and Privacy Commissioner of Ontario (the Commissioner) about certain privacy breaches. This law takes effect **October 1, 2017**.

As a custodian, you must report breaches to the Commissioner in seven categories described in the regulation and summarized below. The categories are not mutually exclusive; more than one can apply to a single privacy breach. If at least one of the situations applies, you must report it. The following is a summary—for the complete wording of the regulation, see the appendix at the end of this document.

It is important to remember that even if you do not need to notify the Commissioner, you have a separate duty to notify individuals whose privacy has been breached under section 12(2) of the act.

### SITUATIONS WHERE YOU MUST NOTIFY THE COMMISSIONER OF A PRIVACY BREACH

#### 1. Use or disclosure without authority

This category covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian. An example would be where a



# Breach Notification, cont'd

## Circumstances where a Privacy Breach must be reported:

- **A health information custodian has reasonable grounds to believe that personal health information in its custody or control was:**
  - **used or disclosed without authority by a person who knew or ought to have known that they were using or disclosing the information without authority.**
    - e.g. person looks at an ex-spouse's medical history for no work related purpose—the “snooping” case.
    - You generally do not need to notify the Commissioner when the breach is accidental, for example, when information is inadvertently sent by email or courier to the wrong person. However, even accidental privacy breaches must be reported if they fall into one of the other categories below.
  - **stolen**
    - e.g. where someone has stolen paper records, or a laptop or other electronic device. Another example would be where patient information is subject to a ransomware or other malware attack, or where the information has been seized through use of a portable storage device.
    - However, you do not need to notify the Commissioner if the stolen information was de-identified or properly encrypted.

# Breach Notification, cont'd

- **after an initial loss or unauthorized use or disclosure, the personal health information was or will be further used or disclosed without authority**
  - e.g. where you learn that an employee wrongfully accessed patient information and subsequently used this information to market products or services or to commit fraud (such as health care or insurance fraud).
  - Even if you did not report the initial incident, you must notify the Commissioner of this situation.
- **loss or unauthorized use or disclosure is part of a pattern of similar losses or unauthorized uses or disclosures of personal health information**
  - e.g. you discover that a letter to a patient inadvertently included information relating to a different patient. Over a few months, the same mistake is repeated several times because an automated process for generating letters has been malfunctioning for some time.
  - You must use your judgment in deciding if a privacy breach is an isolated incident or part of a pattern; take into account, for instance, the time between the breaches and their similarities. Keeping track of privacy breaches in a standard format will help you identify patterns.

# Breach Notification, cont'd

- **The health information custodian is required to give notice to a College of an event described in section 17.1 of the Act that relates to a loss or unauthorized use or disclosure of personal health information.**
  - Bill 119 amended *PHIPA* to require custodians to give notice to a health regulatory college of an event described in section 17.1 of *PHIPA*. The regulation also requires custodians to give notice to the IPC where they are required to give notice to a health regulatory college.
  - Where an employee is a member of a college, you must notify the Commissioner of a privacy breach if:
    - you terminate, suspend or discipline them as a result of the breach
    - they resign and you believe this action is related to the breach
  - Where a health care practitioner with privileges or otherwise affiliated with you is a member of a college, you must notify the Commissioner of a privacy breach if:
    - you revoke, suspend or restrict their privileges or affiliation as a result of the breach
    - they relinquish or voluntarily restrict their privileges or affiliation and you believe this action is related to the breach
  - Similar requirements apply to health care practitioners employed by a board of health.

# Breach Notification, cont'd

- **The health information custodian would be required to give notice to a College, if an agent of the health information custodian were a member of the College, of an event described in section 17.1 of the Act that relates to a loss or unauthorized use or disclosure of personal health information.**
  - Not all employees or other agents of a custodian are members of a college. If an agent is not such a member, you must still notify the Commissioner in the same circumstances that would have triggered notification to a college, had the agent been a member.
- **The health information custodian determines that the loss or unauthorized use or disclosure of personal health information is significant after considering all relevant circumstances, including the following:**
  - i. Whether the personal health information that was lost or used or disclosed without authority is sensitive.
  - ii. Whether the loss or unauthorized use or disclosure involved a large volume of personal health information.
  - iii. Whether the loss or unauthorized use or disclosure involved many individuals' personal health information.
  - iv. Whether more than one health information custodian or agent was responsible for the loss or unauthorized use or disclosure of the personal health information.

# Annual Reports to Commissioner

- Custodians will be required to :
  - start tracking privacy breach statistics as of January 1, 2018
  - provide the Commissioner with an annual report of the previous calendar year's statistics, starting in March 2019.
- The IPC will release detailed guidance on this statistical reporting requirement in fall 2017

# 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



# Interaction of *FIPPA/MFIPPA* and *PHIPA*

# Interaction of *FIPPA/MFIPPA* and *PHIPA*

- *FIPPA/MFIPPA* do not apply to personal health information in the custody or under the control of a health information custodian – *PHIPA*, s. 8(1)
- BUT – *PHIPA* does not limit a person’s right of access under *FIPPA/MFIPPA* if all personal health information is reasonably severed from the record – *PHIPA*, s 8(4)
- *PHIPA* Decision 17:

“If the health information custodian is also an institution subject to *FIPPA* or *MFIPPA*, the requester may have rights of access to both kinds of information under the different statutes (*PHIPA*, section 8(4)). In every case, it is essential to begin with the request, and, where necessary, to clarify with the requester the scope of the request and her intent in making the request.”
- Also see s. 52(3) of *PHIPA* which limits a person’s right of access under *PHIPA* to a record not dedicated primarily to personal health information about the individual to only the personal health information about the individual in the record that can reasonably be severed.



# Detecting and Deterring Unauthorized Access

# Order HO-013

## Nature of the Incident

- Two hospital employees accessed records to market and sell RESPs
- The order found that the hospital did not take steps that were reasonable in the circumstances to safeguard personal health information. The hospital's electronic information system did not:
  - archive activity logs for an appropriate length of time to conduct privacy audits;
  - record all instances of access to personal health information in the user's activity log; and,
  - include search controls – with the result that employees could perform open-ended searches and access personal health information.
- The order also found deficiencies in the hospital's privacy policies, programs and training materials. Significantly, the hospital's policies did not require random audits of all users' activities.

# Detecting and 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 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

# Logging, Auditing, and Monitoring

- Custodians should develop a policy and procedures for logging, auditing and monitoring all electronic information systems containing personal health information.
- Detecting and Deterring Paper describes the content that should be addressed in a health information custodians' policies and procedures regarding logging, auditing and monitoring
- Among other things, the policy and procedures should:
  - require targeted auditing and monitoring to be conducted in response to requests or complaints from individuals regarding the collection, use or disclosure of their personal health information, and whenever an actual or suspected privacy breach is identified;
  - require the custodian to conduct random auditing and monitoring of all collections, uses and disclosures of personal health information by all of their agents.

# Random Audits

- Random auditing and monitoring may include reviews of, for example,
  - all agents who accessed an electronic information system during a specified period of time;
  - all agents who accessed the personal health information of a specific individual, such as a celebrity, politician or other well-known individual, during a specified period of time;
  - all agents who accessed the personal health information of one or more individuals with the same last name as the agent (i.e., family members); and all individuals whose personal health information was access by a specific agent during a specified period of time.
- Third party audit tools are also available which can systematically and automatically analyze access logs and generate reports based upon defined search criteria.

# Discipline by Regulatory Colleges



# Discipline by Regulatory Colleges- *College of Physicians and Surgeons of Ontario v Brooks*

- A physician accessed the electronic records of two individuals to whom he was not providing health care on numerous occasions over the course of a decade – the physician and his wife had a close personal relationship with the two individuals.
- The information accessed included psychiatric care, addictions-related issues and obstetrical care.
- The discipline committee found that the physician committed professional misconduct regarded as disgraceful, dishonourable, or unprofessional.
- The physician was reprimanded and his certificate of registration was suspended for five months.
- The physician was also required to complete six months of individualized instruction in medical ethics pursuant to the terms and conditions placed on his certificate of registration.

# Discipline by Regulatory Colleges- *College of Nurses of Ontario v Smith*

- A nurse, who was in a relationship with another hospital employee, accessed the electronic records of the employee's spouse, to whom she was not providing health care.
- The spouse and employee were in the midst of divorce proceedings; the nurse shared the spouse's personal health information with the employee on several occasions.
- The College found that the nurse committed professional misconduct, failed to meet the standards of practice of the profession and engaged in disgraceful, dishonourable or unprofessional conduct.
- The nurse was reprimanded, her certificate of registration was suspended for six weeks and terms and conditions were imposed on her certificate of registration, including a requirement that the nurse provide a copy of the penalty order together with the notice of the hearing, or if available, the decision and reasons, to any future employers for a period of twelve months.

# 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](http://www.ipc.on.ca)**

**E-mail: [info@ipc.on.ca](mailto:info@ipc.on.ca)**