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

A *PHIPA* Update from the IPC

April 10, 2017

Brian Beamish
Commissioner
Information and Privacy Commissioner of Ontario

OSGOODE PROFESSIONAL DEVELOPMENT | YORK UNIVERSITÉ UNIVERSITY

PHIPA Processes

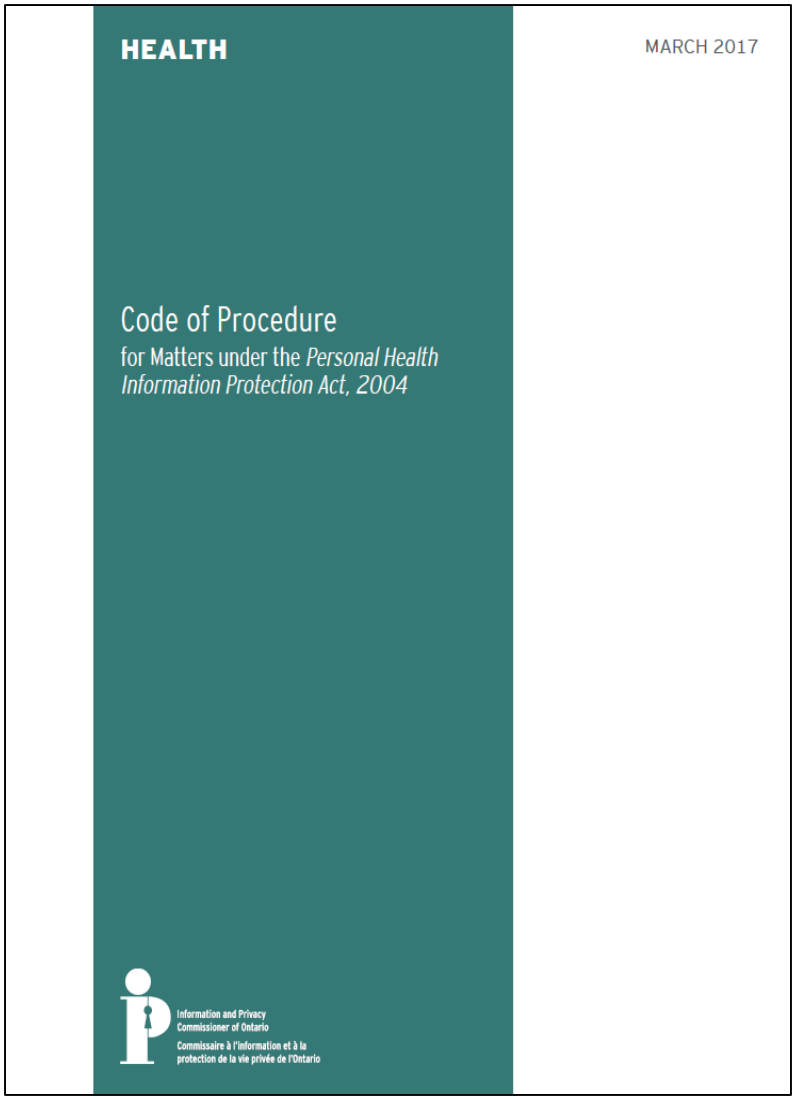
- Internal review of *PHIPA* processes led to some changes
  - Most significant: an increase in the number of public decisions, to provide guidance and increase transparency
  - IPC now issues "*PHIPA* Decisions" which include:
    - Orders
    - Decisions not to conduct a review
    - Decisions following a review, with no orders
    - Interim decisions
  - 29 Decisions and Interim Decisions issued since August 2015

PHIPA Processes – *Cont'd*

- More staff involved in *PHIPA* Decisions
  - *PHIPA* Orders previously written primarily by Commissioner or Assistant Commissioner
  - IPC Adjudicators and Investigators to write more decisions
- Code of Procedure for all *PHIPA* files has been released, with additional Practice Directions
  - New or revised Practice Directions deal with:
    - new *PHIPA* complaint forms
    - how to respond to access requests
    - IPC practice on naming parties in public decisions

New *PHIPA* Code of Procedure

- New code is the result of an internal review of our *PHIPA* processes
- Came into force on March 15, 2017, and applies immediately to all IPC files under *PHIPA*
- Replaces previous code of procedure for access/correction complaints; now a single comprehensive code applicable to all matters arising under *PHIPA*
- New practice directions will provide guidance to parties exercising their rights and complying with their obligations under this new code and *PHIPA*



PHIPA Processes – *cont'd.*

- What has not changed:
  - efforts to reach early resolution of complaints
  - 70 per cent of access/correction complaints and 60 per cent of collection/use/disclosure complaints are settled through mediation
- Almost all self-reported breaches are resolved at Intake

Goal of IPC Investigations

- When health information custodians (custodian) self-report privacy breaches, IPC determines whether response of custodian was adequate, including:
  - notice to affected patients
  - disciplinary response
  - addressing systemic issues
    - auditing/logging
    - training
    - confidentiality agreements
    - privacy warnings on electronic systems
- Determine whether to refer to Attorney General for prosecution

Some *PHIPA* Decisions

- Interaction between *FIPPA* and *PHIPA* access provisions: *PHIPA* Decision 17
- What is a reasonable search in response to an access request? *PHIPA* Decision 18
- Can a complaint be made about a refusal to disclose? *PHIPA* Decisions 19, 20, 21, 22
- Approach to issuing an interim order: *PHIPA* Decision 23
- Decision not to conduct a review: *PHIPA* Decision 32
- Duty to correct health records: *PHIPA* Decisions 36, 37, 39, 41
- Alleged breach of collection, use and disclosure provisions of *PHIPA* by hospital: *PHIPA* Decision 38

Unauthorized Access

- The IPC receives about 300-350 complaints per year about privacy breaches in the health sector
- Most are caused by carelessness, such as the loss or theft of portable devices or misdirected emails or faxes
- Two or three cases per month of intentional “snooping,” unauthorized access to records of PHI
- Very few snooping cases have resulted in orders
    - custodians (mainly hospitals) take these cases seriously and take steps to address the IPC’s concerns about systemic issues that contribute to snooping

Examples of Unauthorized Access – Education and Quality Improvement

- There have been a number of instances of unauthorized access where custodians or agents have accessed PHI claiming it was for:
  - educational purposes
  - improving the quality of the health care they provide

Challenges in Establishing "Unauthorized" Access

- Demonstrating such accesses are unauthorized may be difficult where the custodian does not:
  - have clear policies specifying the purposes for which access is and is not permitted
  - have procedures that must be followed when accessing information for purposes other than providing care
  - inform agents when access is permitted and is not permitted, through training, notices, flags in electronic systems, agreements, etc.

Doctors with Privileges

- Hospital agents may have off-site practices where they, and their employees, have access to PHI on the hospital's electronic information system. For example, a doctor with privileges at a hospital may operate a clinic where he/she employs administrative staff
- Where a doctor employs private staff with access to PHI in the custody or control of a hospital, both the hospital and the doctor are responsible for the activities of the employee

Doctors with Privileges *(Cont'd)*

- The hospital, the doctor, and the doctor's staff should clearly specify, in writing, their respective roles and responsibilities:
    - who is a custodian,
    - who is an agent of the hospital, and
    - who is an agent of the doctor
- Clarifying roles and responsibilities will ensure that there is appropriate training, confidentiality agreements are signed, policies and procedures are followed, etc.

Update on HO-013 (Rouge Valley)

- ***PHIPA* Order HO-013**
  - Rouge Valley Health System reported that two employees accessed records to market and sell RESPs
  - IPC investigated and concluded that the hospital did not take reasonable steps to protect PHI
  - Among other things, IPC ordered hospital to change its electronic information systems to ensure the ability to audit all instances of access to PHI

Update on HO-013 (Rouge Valley) – *Cont'd*

- The hospital appealed HO-013 to the Divisional Court.
- After discussions between the hospital and the IPC, the hospital withdrew its appeal:
  - The hospital and the IPC would cooperate on strategies to implement the Order relating to its electronic information systems in a manner that was compliant with *PHIPA* in the view of the IPC
  - The IPC and the hospital would agree on a work plan setting out a time frame for the actions noted in the plan

Update on HO-013 (Rouge Valley) – *Cont'd*

- The hospital identified electronic systems containing PHI
- The hospital will buy software that performs logging and auditing
- The IPC and the hospital agreed on the systems that will be covered by the software
- The software will not be deployed to systems that are due to retire soon, to which limited staff have access, or which only conduct real-time monitoring and do not record PHI
- A schedule has been developed for deployment
- Will apply to both "new" entities

Most Recent Prosecution Under *PHIPA*

- A Masters of Social Work student, who was on an educational placement with a family health team in Central Huron, has been ordered to pay a $20,000 fine and a $5,000 victim surcharge for accessing PHI without authorization
- This is the highest fine to date for a health privacy breach in Canada
- The IPC was advised, in March 2015, that the student was illegally accessing the records of family, friends, local politicians, staff of the clinic and other individuals
- Following an investigation, the IPC referred the matter to the Attorney General of Ontario

Most Recent Prosecution Under *PHIPA* *(Cont'd)*

- The student pled guilty to willfully accessing the PHI of five individuals
- As part of her plea, she agreed that she accessed the PHI of 139 individuals without authorization between September 9, 2014 and March 5, 2015
- This is the fourth person convicted under *PHIPA*. Two radiation therapists at the University Health Network and a registration clerk at a regional hospital were previously convicted under *PHIPA*

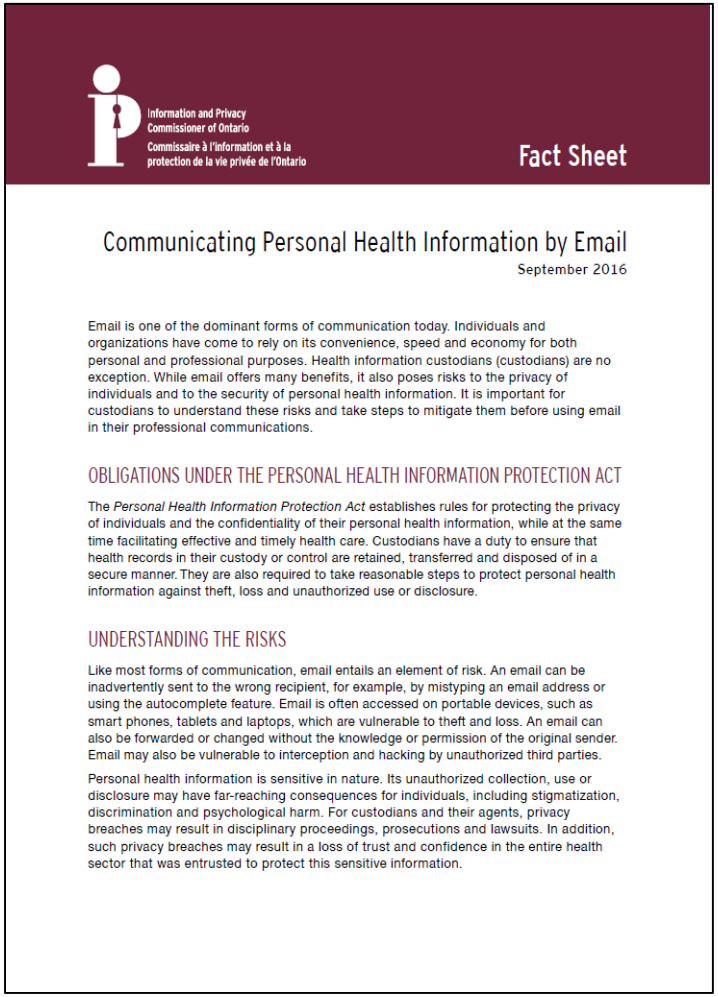
Most Recent Prosecution Under *PHIPA* *(Cont'd)*

- *"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 heath 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

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
- For emailing PHI between custodians, IPC expects encryption, barring exceptional circumstances



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.

OSGOODE PROFESSIONAL DEVELOPMENT
OSGOODE HALL LAW SCHOOL
YORK UNIVERSITÉ UNIVERSITY

Communicating PHI by Email – *Cont'd*

- 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
- 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

Data Analytics

- Big Data Analytics represents a shift in how we think about and use data:
  - New combinations of data may contain useful, but hidden patterns and insights
  - Advanced analytics can discover these insights
- The sharing, linking and analysis of data can provide new insights, for such purposes as:
  - policy development
  - system planning
  - resource allocation
  - performance monitoring
  - sometimes referred to as “data integration”

Privacy Risks of Big Data

- Generation of new PI not collected directly from the individual
- Use of poorly selected data sets that:
  - lack information/are incomplete
  - contain incorrect or outdated information
  - disproportionately represent certain populations
- Incorporation of implicit or explicit biases
- Generation of pseudo-scientific insights that assume correlation equals causation
- Lack of knowledge/transparency regarding the inner “logic” of the system
- *If not designed properly, can result in uses of PI that may be unexpected, invasive and discriminatory*

Data Analytics in Health Care *(Cont'd)*

- *PHIPA* recognizes the value of health research and analysis
- custodians can collect, use and disclose PHI for purposes beyond the provision of health care, such as:
  - research with or without consent
  - use for risk and error management and activities to improve or maintain the quality of care and related programs and services
  - disclosure to a prescribed person that compiles or maintains a registry to facilitate or improve the provision of health care
  - disclosure to a prescribed entity for analysis or planning, managing and evaluating the health system
- Under Bill 119, the minister is permitted to collect PHI from the provincial electronic health record to fund and plan health services and detect, monitor or prevent fraud

Oversight For Research Without Consent

- *PHIPA* requires a research plan to be approved by a research ethics board (REB)
- The REB is required to consider all relevant matters, including:
    - Whether the research requires PHI
    - Whether obtaining consent would be impractical
    - The public interest in the research and the protection of privacy
    - The adequacy of safeguards to protect privacy and confidentiality
- If the research is not conducted on behalf of a custodian, there must be an agreement that sets out the conditions and restrictions relating to the use, security, disclosure, return or disposal of the PHI
- Researchers must also comply with certain requirements, including notifying the custodian of a breach of *PHIPA* or the agreement

Oversight of Prescribed Persons and Entities

- Prescribed persons and prescribed entities must:
  - Comply with the restrictions on use and disclosure in *PHIPA*
  - Have their privacy policies, procedures and practices reviewed and approved by my office every three years
  - Comply with the *Manual for Review and Approval of Prescribed Persons and Prescribed Entities,* developed by my office
- The *Manual* sets out detailed policies, procedures and practices that must be implemented and the privacy and security indicators that must be reported on

Oversight of Collection by the Minister

- In order for the Minister to be permitted to collect PHI from the provincial electronic health record:
  - The Lieutenant Governor in Council must prescribe not more than one unit of the Ministry to collect the PHI on the Minister's behalf
  - The PHI must be de-identified and thereafter only de-identified information may be used or disclosed, subject to limited exceptions
  - PHI may only be used where there are reasonable grounds to believe there has been inappropriate receipt of a payment, service or good that is health-related or prescribed
  - The PHI may only be used by one unit of the ministry prescribed by the Lieutenant Governor in Council
  - The prescribed units must put in place practices and procedures approved by my office

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