The Latest Happenings from the IPC

Brendan Gray, Health Law Counsel

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

2017 PHIPA Connections Summit

December 6, 2017

DISCLAIMER

THIS PRESENTATION IS:

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

Topics

1. Background to IPC's *PHIPA* Processes
2. *PHIPA* Beyond Health Information Custodians
3. Health Information Custodians after Bankruptcy or Death
4. *PHIPA* Access to Raw Data
5. Communication of Personal Health Information by Email
6. Breach Notification and Annual Reporting to IPC under Bill 119 – *Health Information Protection Act, 2016*

IPC's *PHIPA* Processes

PHIPA Processes

- Internal review of IPC's *PHIPA* processes led to 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
  - 45 Decisions and Interim Decisions issued since August 2015
  - More staff involved in *PHIPA* Decisions
    - *PHIPA* Orders previously written primarily by Commissioner or Assistant Commissioner
    - IPC Adjudicators and Investigators to write more decisions

HEALTH

MARCH 2017

Code of Procedure

for Matters under the *Personal Health Information Protection Act, 2004*

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

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

PHIPA Beyond Health Information Custodians

PHIPA Decision 56

- Section 34 of the *PHIPA* sets out rules relating to the collection, use, and disclosure of health numbers by a person who is neither a health information custodian nor acting as an agent of a health information custodian.
- A "health number" is a subcategory of "personal health information" and is defined in section 2 of *PHIPA* as: "the number, the version code or both of them assigned to an insured person within the meaning of the *Health Insurance Act* by the General Manager within the meaning of that Act".
- The *PHIPA* also limits when a person (including a health information custodian) may require the production of another person's health card.

PHIPA Decision 56, cont'd

- Among other things, *PHIPA* provides that a person who is neither a health information custodian nor acting as an agent of a health information custodian shall not collect, use or disclose another person's health number except "for purposes related to the provision of provincially funded health resources to that other person" – with some exceptions.
- "provincially funded health resource" means a service, thing, subsidy or other benefit funded, in whole or in part, directly or indirectly by the Government of Ontario, if it is health related or prescribed.

PHIPA Decision 56, cont'd

- The IPC learned that an insurance company was collecting health numbers through its application process for purchasing supplementary health insurance plans.
- The IPC also learned that the insurance company was collecting health numbers at the time of claim in relation to emergency medical travel benefits.
- The IPC opened this file and contacted the insurance company.
- The insurance company took the position that it collects, uses, and discloses health numbers for purposes related to the provision of provincially funded health resources.

PHIPA Decision 56, cont'd

- Supplementary health insurance plans: the insurance company initially submitted that it collects health numbers in order to co-ordinate payments with the provincial health plan.
- However, the insurance company later clarified that it did not require Ontario health numbers to co-ordinate supplementary health insurance plan payments. Rather, it required confirmation that OHIP had paid its portion of a benefit before it paid the balance to the insured, subject to the policy limits.
- Emergency medical travel benefits: the insurance company submitted that it collects health numbers for the purpose of co-ordinating and administering emergency travel insurance benefit claims.
- The insurance company explained that the health number is disclosed to Ontario hospitals as part of repatriating patients from another country or, as the insurance company is a secondary payer, to obtain reimbursement from the Ministry of Health and Long-Term Care for the portion of the claim that OHIP would fund.

PHIPA Decision 56, cont'd

- IPC found that a collection, use, or disclosure of a health number will only be "related to the provision of provincially funded health resources" where the health number is collected, used, or disclosed for the purposes of the provincial funding of health resources, or directly obtaining those health resources.
- Supplementary health insurance plans: the IPC found that the collection and use of the health number on application forms for supplementary health insurance plans does not relate to provincial funding of the health resource, but related to the portion of the health resource paid for by the individual (and their insurer). This was not permitted by section 34 of *PHIPA*
- Emergency medical travel benefits: The IPC found that obtaining reimbursement from OHIP for the portion of the claim that is OHIP funded, and arranging bed to bed repatriations, were done for the purposes of the provincial funding of the health resource, or for directly obtaining that resource. These were permitted by section 34.
- No review was warranted because the insurance company had, among other things, discontinued the collection of health numbers on both paper and electronic applications, and deleted all health numbers from its administrative system.

PHIPA Decision 49

- Section 49(1) of *PHIPA* sets out restrictions on recipients who are not health information custodians but who receive personal health information from health information custodians. Section 49(1) prohibits a recipient from using or disclosing the personal health information "for any purpose", except where the use and/or disclosure is:
  - permitted or required by law;
  - for the purpose for which the health information custodian was authorized to disclose the information under the Act;
  - for the purpose of carrying out a statutory or legal duty; or,
  - subject to prescribed exceptions and additional requirements, if any.
- In this case, a lawyer reported to the IPC that her client, a physician, had received an email from a former patient containing an image of a computer screen in the physician's examination room.
- The physician determined that the image showed the daily schedule of the physician's EMR, containing the personal health information of 72 individuals. The physician speculated that the respondent obtained the image by photographing the screen immediately after either he or another staff member left the examination room and prior to the automatic log-off being engaged.

PHIPA Decision 49, cont'd

- The former patient refused to delete the image.
- IPC commenced a review with respect to whether the former patient had contravened, or was about to contravene, section 49(1) of *PHIPA*.
- IPC opened a separate file to address the physician's obligations to ensure the security of personal health information.
- The former patient said could make the "information public if necessary" and later submitted that the image was taken to "document a serious breach of patient privacy and confidentiality that occurred when both his and dozens of other patients' personal health information was openly displayed on a computer screen that either the physician or one of his staff failed to log-off"

PHIPA Decision 49, cont'd

- The former patient advised that he did not plan to share the image with anyone other than his lawyer for the purpose of bringing a legal action against the physician.
- IPC found that there were no purposes for which the physician, (as the health information custodian) was authorized to disclose the personal health information to the former patient.
- So the former patient could not use or disclose the image except as permitted or required by law or for the purpose of carrying out a statutory or legal duty
- No evidence former patient had statutory or legal duty – analysis focused on whether his uses and potential disclosures were permitted by law.

PHIPA Decision 49, cont'd

- The former patient took the photograph approximately 18 months before PHIPA Decision 49 was released.
- There was no evidence to suggest that he had commenced any legal proceeding, that he had retained a lawyer for that purpose, nor that anyone else had commenced a proceeding with respect to this matter (other than the IPC's investigation).
- No evidence former patient needed the image to prove this privacy breach, as neither the fact of the breach nor the scope of the breach could reasonably be in dispute – physician already notified patients of breach.
- Physician undertook to retain a copy of the image and to comply with any order of a court or tribunal of competent jurisdiction requiring disclosure.
- IPC found former patient had used the image without authorization and ordered the Respondent to securely dispose of the personal health information of other individuals in the image.

Health Information Custodians after Bankruptcy or Death

PHIPA Decisions 23 and 28

- The IPC was advised that records of personal health information had been abandoned in the wake of the bankruptcy of three corporations that operated four clinics providing health services in the GTA.
- Records were left in premises formerly leased by the bankrupt corporations.
- IPC issued a notice of review to the three bankrupt corporations, their trustee in bankruptcy, the landlords for the four clinics leased by the bankrupt corporations, and four directors and/or officers of the bankrupt corporations

PHIPA Decisions 23 and 28, cont'd

- Section 3(7) of the regulation to *PHIPA* provides that "Every person who, as a result of the bankruptcy or insolvency of a health information custodian, obtains complete custody or control of records of personal health information held by the health information custodian, is prescribed as the health information custodian with respect to those records."
- The IPC sought representations from the bankruptcy trustees and the landlords on the application of that section to their possession of the abandoned records.
- IPC also issued an interim order to one landlord to secure records pending completion of review.

PHIPA Decisions 23 and 28, cont'd

- Primary purpose of this review was to determine which, if any, of the named respondents was responsible for ensuring the security of the abandoned records, and ensuring that individuals will be able to exercise their right of access to their health records.
- The IPC was subsequently advised that all patient files abandoned by the three bankrupt corporations had been secured by a combination of *Regulated Health Professions Act* colleges, a health information custodian who subsequently leased one of the clinic locations, and members of *RHPA* colleges who provided health services at these locations.
- Steps were taken to ensure that individuals would be able to access their records and would be notified of where they are now retained.
- Not necessary to continue with review, no order issued.

PHIPA Decision 29

- Former patient of a deceased doctor complained about the actions of a medical records storage company holding the records of the deceased doctor.
- He complained that he had the right to obtain the original paper health records compiled by his family physician, and that the medical records storage company wrongfully destroyed paper health records after they were converted into electronic format.
- Section 3(12) of *PHIPA* provides:

> If a health information custodian dies, the following person shall be deemed to be the health information custodian with respect to records of personal health information held by the deceased custodian until custody and control of the records, where applicable, passes to another person who is legally authorized to hold the records:
>
> 1. The estate trustee of the deceased custodian.
>
> 2. The person who has assumed responsibility for the administration of the deceased custodian's estate, if the estate does not have an estate trustee.

PHIPA Decision 29, cont'd

- Deceased doctor's estate trustee entered into contract with medical records storage company.
- The medical records storage company submitted that the estate trustee of the deceased physician was not a health information custodian. The company stated that the estate trustee had retained it as an "'agent', acting as sole custodian" of the records.
- The complainant submitted that the estate trustee is a health information custodian, but also submitted that the medical records storage company was not an agent of the health information custodian.
- The complainant stated that the estate trustee may only "assign her responsibilities as health information custodian to [the medical records storage company]" with the consent of his family.

PHIPA Decision 29, cont'd

- IPC found that the estate trustee was, and remained, the health information custodian of the records. The agreement with the medical records storage company was not, by itself, enough to relieve the health information custodian of responsibility.
- IPC found that medical records storage company was not a health information custodian (not listed in section 3 of *PHIPA*) but was an agent of the estate trustee. IPC found that consent was not required to delegate to an agent.
- IPC found that:
  - *PHIPA* did not require the medical records storage company to provide the complainant with the original paper records formerly held by his physician, and
  - these records were not his property pursuant to regulations under the *Medicine Act* addressing what happens to medical records when a physician dies.

PHIPA Decision 29, cont'd

- Lastly, the IPC found that the ability to scan a paper record into electronic format is necessarily ancillary to the ability to keep electronic records of personal health information. *PHIPA* plainly permits health information custodians to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information.
- As such, this use was permitted without consent.
- The IPC noted that having accurate and complete records of personal health information facilitates the effective provision of health care.
- *PHIPA* should not be interpreted so that health information custodians are unable to upgrade or improve the format in which their records are retained.

PHIPA Access to Raw Data

PHIPA Decision 52

- After being given access to the contents of his central health record at a hospital, including diagnostic images, an individual sought access to all the underlying electronic data about him held by the hospital, in its native, industry-standard electronic format.
- The hospital refused to provide the complainant with the underlying raw data from which the information in the health record was derived, such as in medical devices or databases associated with each electronic system.
- Decision dealt with the right of access to raw data.

PHIPA Decision 52, cont'd

- *PHIPA* provides individuals with a right of access to records of personal health information about them in the custody or control of a health information custodian. "Record" is defined in section 2 of PHIPA:

> "record" means a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record;

- Right of access may be limited if a record is not dedicated primarily to the information of the person requesting access:

> 52(3) Despite subsection (1), if a record is not a record dedicated primarily to personal health information about the individual requesting access, the individual has a right of access only to the portion of personal health information about the individual in the record that can reasonably be severed from the record for the purpose of providing access.

- The hospital submitted that, in its view, the complainant was asking for data, not information. It stated that permitting access to raw data in native format goes beyond a plain reading of *PHIPA*. The hospital submitted that accessing raw data in its native format may require a translating program or mechanism from a vendor so as to render the data readable.

PHIPA Decision 52, cont'd

- The IPC found that the definition of a "record" of "personal health information" was broad enough to encompass "data" within an electronic system.
- The hospital did not dispute that information within these systems is associated with identifiable patients, through patient names or other identifiers.
- Given this, there was no basis for distinguishing between identifying "data" and "information".
- However, the IPC also found that the electronic databases in which the complainant's information was found were not dedicated primarily to his information. Each of them pooled his information together with that of many other patients.

PHIPA Decision 52, cont'd

- Where a record is not dedicated primarily to the personal health information of the individual seeking access, the right of access applies only to the individual's personal health information that can be reasonably severed from the record.
- The IPC distinguished between data that could be extracted by the hospital and data that the hospital could not extract through its own efforts (requiring the assistance of vendors). IPC noted that some of the data the complainant seeks is not reasonably available even to the hospital. It is data used in machine processing and not intended to be used by hospital staff.
- The IPC concluded that where the extraction of the complainant's information can be done through the development of conventional custom queries by hospital staff, based on information in reporting views available to the hospital, the complainant's information can be reasonably severed for the purpose of section 52(3).
- In short, complainant had a right of access to data about him that may be extracted through custom software queries against reporting views.
- This right of access was subject to the hospital's right to reasonable cost recovery (provided it issues a fee estimate) in connection with this work.

Communication of Personal Health Information by Email

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

Fact Sheet

Communicating Personal Health Information by Email

September 2016

Email is one of the dominant forms of communication today. Individuals and organizations have come to rely on its convenience, speed and economy for both personal and professional purposes. Health information custodians (custodians) are no exception. While email offers many benefits, it also poses risks to the privacy of individuals and to the security of personal health information. It is important for custodians to understand these risks and take steps to mitigate them before using email in their professional communications.

OBLIGATIONS UNDER THE PERSONAL HEALTH INFORMATION PROTECTION ACT

The *Personal Health Information Protection Act* establishes rules for protecting the privacy of individuals and the confidentiality of their personal health information, while at the same time facilitating effective and timely health care. Custodians have a duty to ensure that health records in their custody or control are retained, transferred and disposed of in a secure manner. They are also required to take reasonable steps to protect personal health information against theft, loss and unauthorized use or disclosure.

UNDERSTANDING THE RISKS

Like most forms of communication, email entails an element of risk. An email can be inadvertently sent to the wrong recipient, for example, by mistyping an email address or using the autocomplete feature. Email is often accessed on portable devices, such as smart phones, tablets and laptops, which are vulnerable to theft and loss. An email can also be forwarded or changed without the knowledge or permission of the original sender. Email may also be vulnerable to interception and hacking by unauthorized third parties.

Personal health information is sensitive in nature. Its unauthorized collection, use or disclosure may have far-reaching consequences for individuals, including stigmatization, discrimination and psychological harm. For custodians and their agents, privacy breaches may result in disciplinary proceedings, prosecutions and lawsuits. In addition, such privacy breaches may result in a loss of trust and confidence in the entire health sector that was entrusted to protect this sensitive information.

Communicating by Email

- *PHIPA* sets out rules for protecting the privacy of patients and the confidentiality of their personal health information (PHI), while facilitating effective and timely care.
- Any communication of PHI involves risk, but communicating PHI by email has its own set of unique risks.
- These risks must be considered by health information custodians (custodians) and their agents in order to protect the privacy and confidentiality of patients.

Technical, Physical and Administrative Safeguards

- Custodians are required to implement technical, physical and administrative safeguards to protect PHI.
- Technical safeguards include:
  - encrypting portable devices
  - strong passwords
  - firewalls and anti-malware scanners
- Physical Safeguards:
  - restricting access by locking server rooms where email is retained
  - keeping portable devices in secure location

Technical, Physical and Administrative Safeguards

- Administrative safeguards:
  - notice in emails that information is confidential
  - providing instructions for when email is received in error
  - communicate by professional vs personal accounts
  - confirming recipient email address is current
  - checking that email address is typed correctly
  - restricting access to email system and content on need-to-know basis
  - informing individuals of email changes
  - acknowledging receipt of emails
  - recommending that recipients implement these safeguards

Email Between Custodians

- The IPC expects emailing of PHI among custodians to be secured by use of encryption.
- There may be exceptional circumstances where communication of PHI between custodians through encrypted email may not be practical (i.e. in urgent circumstances where the PHI is needed to minimize a significant risk of serious bodily harm).
- Custodians should look to their regulatory colleges for applicable guidelines, standards or regulations.

Email Between Custodians and Patients

- Where feasible, custodians should use encryption for communicating with their patients.
- Where not feasible, custodians should consider whether it is reasonable to communicate through unencrypted email.
  - Are there alternative methods?
  - Is the PHI urgently needed to minimize a significant risk of serious bodily harm?
  - Would the patient expect you to communicate with him/her in this manner?
  - How sensitive is the PHI to be communicated?
  - How much and how frequently will be PHI be communicated?

Policy, Notice and Consent

Policy

- Custodians are expected to develop and implement a written policy for sending and receiving PHI by email.

Notice and Consent

- Custodians are expected to notify their patients about this policy and obtain their consent prior to communicating by means of email that is not encrypted.
- Consent may be provided in verbally or in writing.

Data Minimization, Retention and Disposal

Data Minimization

- Custodians have a duty to limit the amount and type of PHI included in an email.

Retention and Disposal

- Custodians are required to retain and dispose of PHI in a secure manner.
- PHI must only be stored on email servers and portable devices for as long as is necessary to serve the intended purpose.

Training and Privacy Breach Management

Training and Education

- Comprehensive privacy and security training is essential for reducing the risk of unauthorized collection, use and disclosure of PHI.

Privacy Breach Management

- Custodians are expected to have a privacy breach management protocol in place that identifies the reporting, containment, notification, investigation and remediation of actual and suspected privacy breaches.

Bill 119 - *Health Information Protection Act:*

Breach Notification and Annual Reports

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 to the Commissioner

- 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 a breach must be reported to the Commissioner

SEPTEMBER 2017

GUIDELINES FOR THE HEALTH SECTOR

Reporting a Privacy Breach to the Commissioner

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

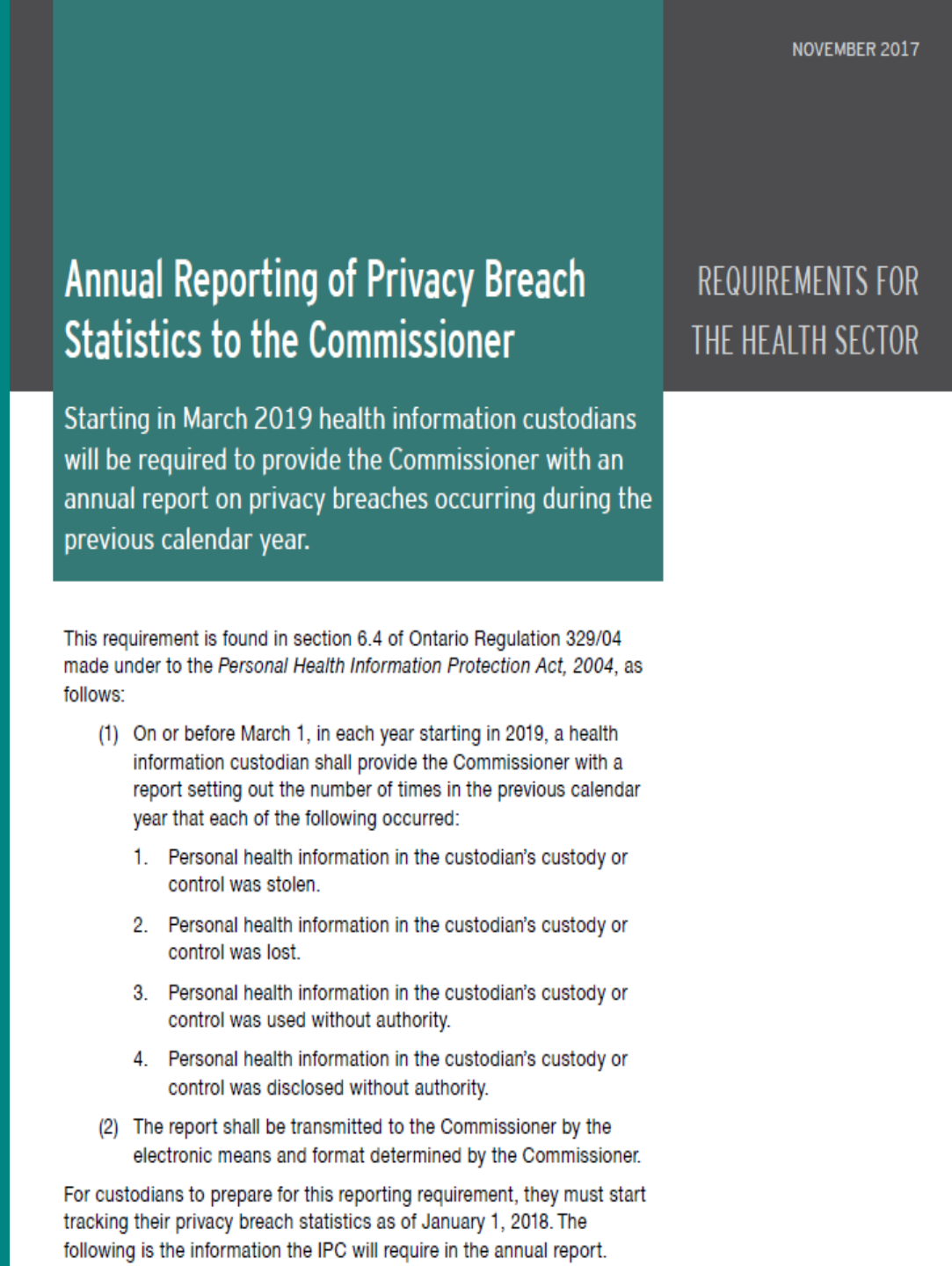
1. Use or disclosure without authority

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

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

Annual Reports to the 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 recently released a guidance document on this statistical reporting requirement



NOVEMBER 2017

Annual Reporting of Privacy Breach Statistics to the Commissioner

REQUIREMENTS FOR THE HEALTH SECTOR

Starting in March 2019 health information custodians will be required to provide the Commissioner with an annual report on privacy breaches occurring during the previous calendar year.

This requirement is found in section 6.4 of Ontario Regulation 329/04 made under to the *Personal Health Information Protection Act, 2004*, as follows:

(1) On or before March 1, in each year starting in 2019, a health information custodian shall provide the Commissioner with a report setting out the number of times in the previous calendar year that each of the following occurred:

1. Personal health information in the custodian's custody or control was stolen.
2. Personal health information in the custodian's custody or control was lost.
3. Personal health information in the custodian's custody or control was used without authority.
4. Personal health information in the custodian's custody or control was disclosed without authority.

(2) The report shall be transmitted to the Commissioner by the electronic means and format determined by the Commissioner.

For custodians to prepare for this reporting requirement, they must start tracking their privacy breach statistics as of January 1, 2018. The following is the information the IPC will require in the annual report.

QUESTIONS?

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

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965