TACKLING PRIVACY BREACHES FOR HEALTH CARE PROVIDERS

Manuela Di Re

Director of Legal Services and General Counsel

Information and Privacy Commissioner of Ontario

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

Privacy Law Summit 2019

Ontario Bar Association

April 3, 2019

Breach Notification Obligations

A custodian must:

- *Notify the affected individual* at the first reasonable opportunity if personal health information is stolen, lost or used or disclosed without authority
- *Notify the Information and Privacy Commissioner of Ontario (IPC)* if the circumstances surrounding the theft, loss or unauthorized use or disclosure meet the prescribed requirements
- *Provide the IPC* with a statistical report on or before March 1st each year, starting in 2019, of breaches in the previous calendar year

POINT IN TIME REPORTING

Point-In-Time Breach Reporting

A custodian must notify the IPC of a theft, loss or unauthorized use or disclosure in the following circumstances:

1. Use or disclosure without authority
2. Stolen information
3. Further use or disclosure without authority after a breach
4. Pattern of similar breaches
5. Disciplinary action against a college member
6. Disciplinary action against a non-college member
7. Significant breach

Guidance Document

- The IPC has published a guidance document providing more detail about point in time reporting

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

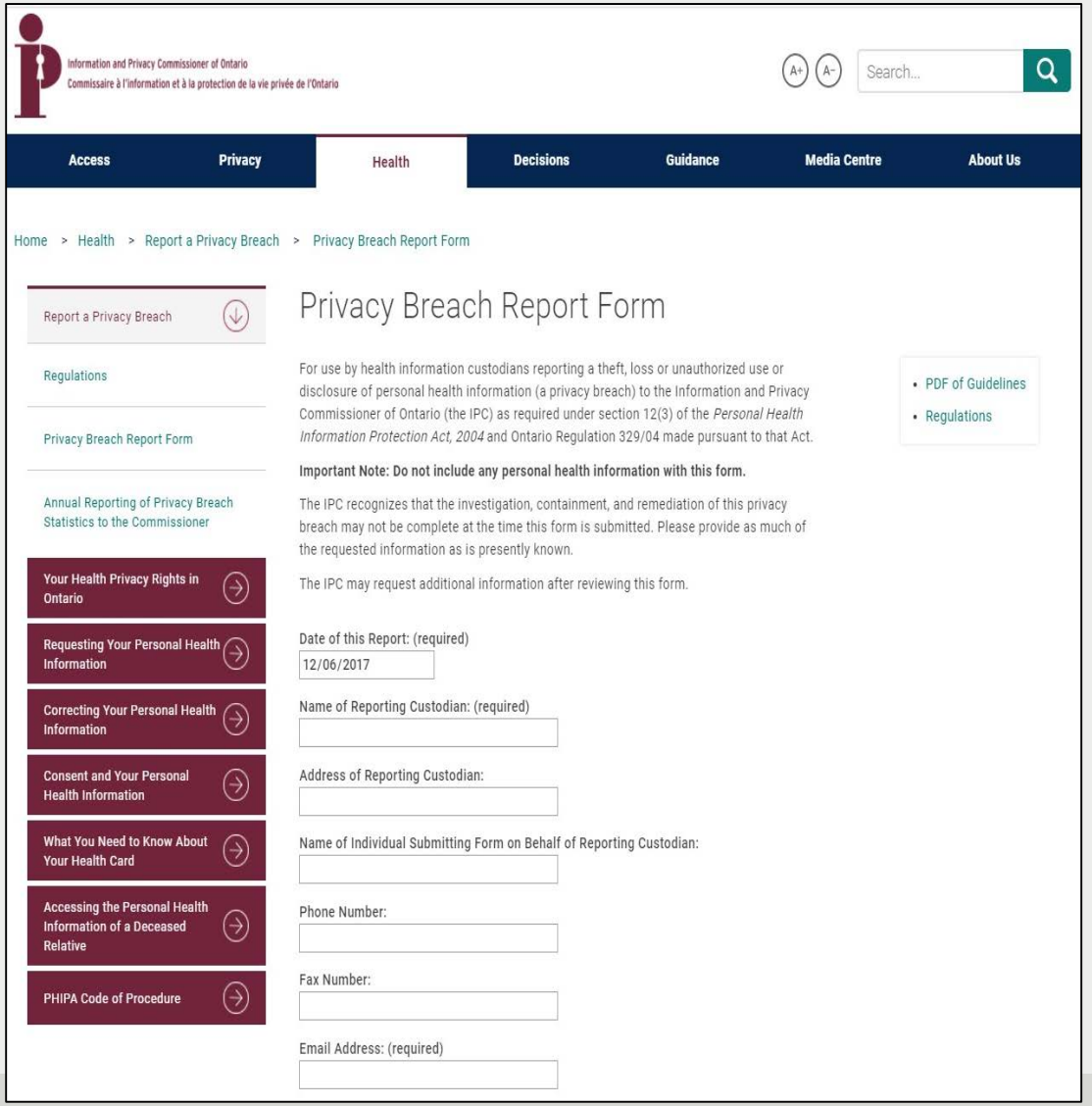
Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

IPC Privacy Breach Online Report Form

Although you can report point in time breaches by mail or fax, the IPC recommends you use our online report form.

You will be asked to provide:

- a description of the breach
- steps taken to contain the breach
- steps taken to notify affected individuals
- steps taken to investigate and remediate the breach



What to Expect

Intake Stage

- File may be closed quickly if the information provided is complete and the IPC is satisfied with steps taken
- Analyst may contact the custodian to clarify the facts and issues
- The goal is to informally resolve any issues raised by the breach

Investigation/Mediation Stage

- IPC investigates whether the custodian has adequately responded to breach, and any additional issues raised by the breach
- File may be closed by decision or mediator's report
- Where a complainant is involved, IPC attempts to find a consensual resolution
- If not resolved or closed, the file is sent to adjudication

What to Expect

Adjudication

- IPC reviews facts of case, may close case without a review, or start a review
- If a Notice of Review is issued, the parties will be asked to provide further details and facts related to the matters at issue
- Adjudicator will issue a decision to resolve all the issues, which may include orders and recommendations

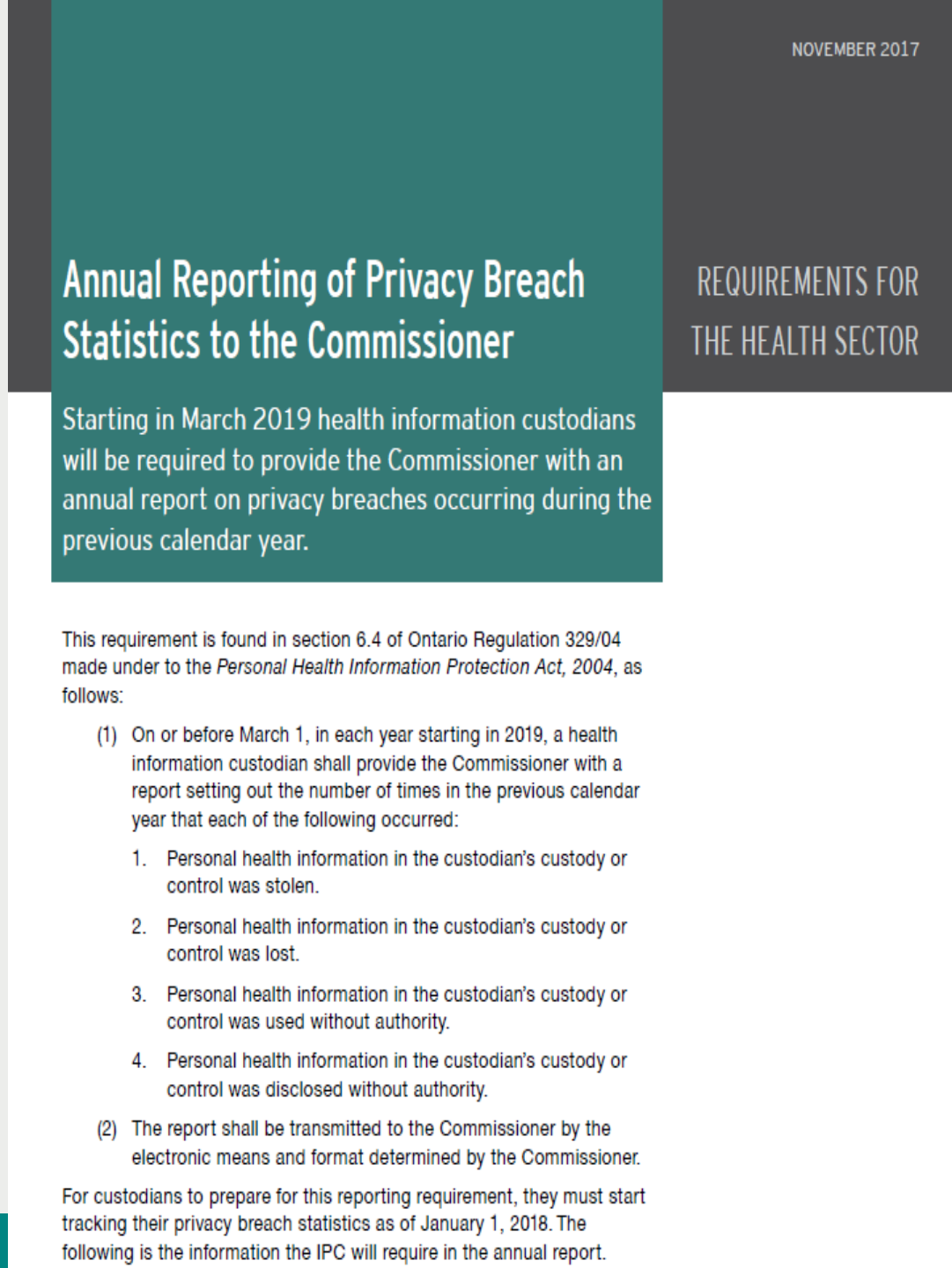
ANNUAL STATISTICAL REPORTING

Annual Statistical Reports to the Commissioner

- Custodians are required to provide the IPC with an annual report of the previous calendar year's statistics (beginning on March 1, 2019)
- The annual report must set out the number of times in the prior calendar year that personal health information in the custodian's custody or control was:
  - stolen
  - lost
  - used without authority
  - disclosed without authority
- Statistics were collected through the IPC's Online Statistics Submission website - https://statistics.ipc.on.ca/web/site/login

Guidance Document – Annual Statistical Report

- The IPC has released a guidance document about the annual statistical reporting requirement
- The guidance document outlines the specific information that must be reported for each category of breach



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:

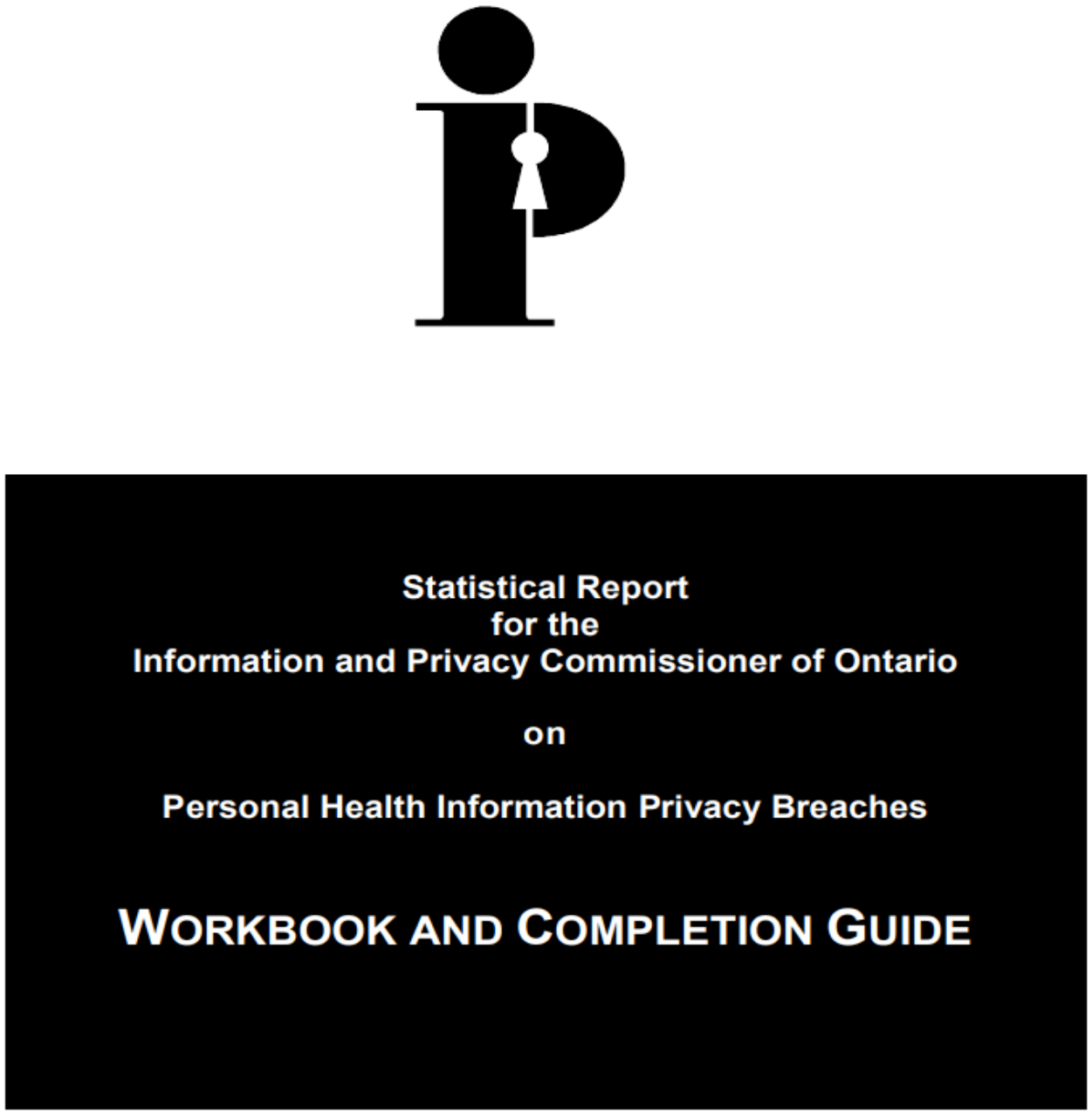
1. Personal health information in the custodian's custody or control was stolen.
2. Personal health information in the custodian's custody or control was lost.
3. Personal health information in the custodian's custody or control was used without authority.
4. Personal health information in the custodian's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

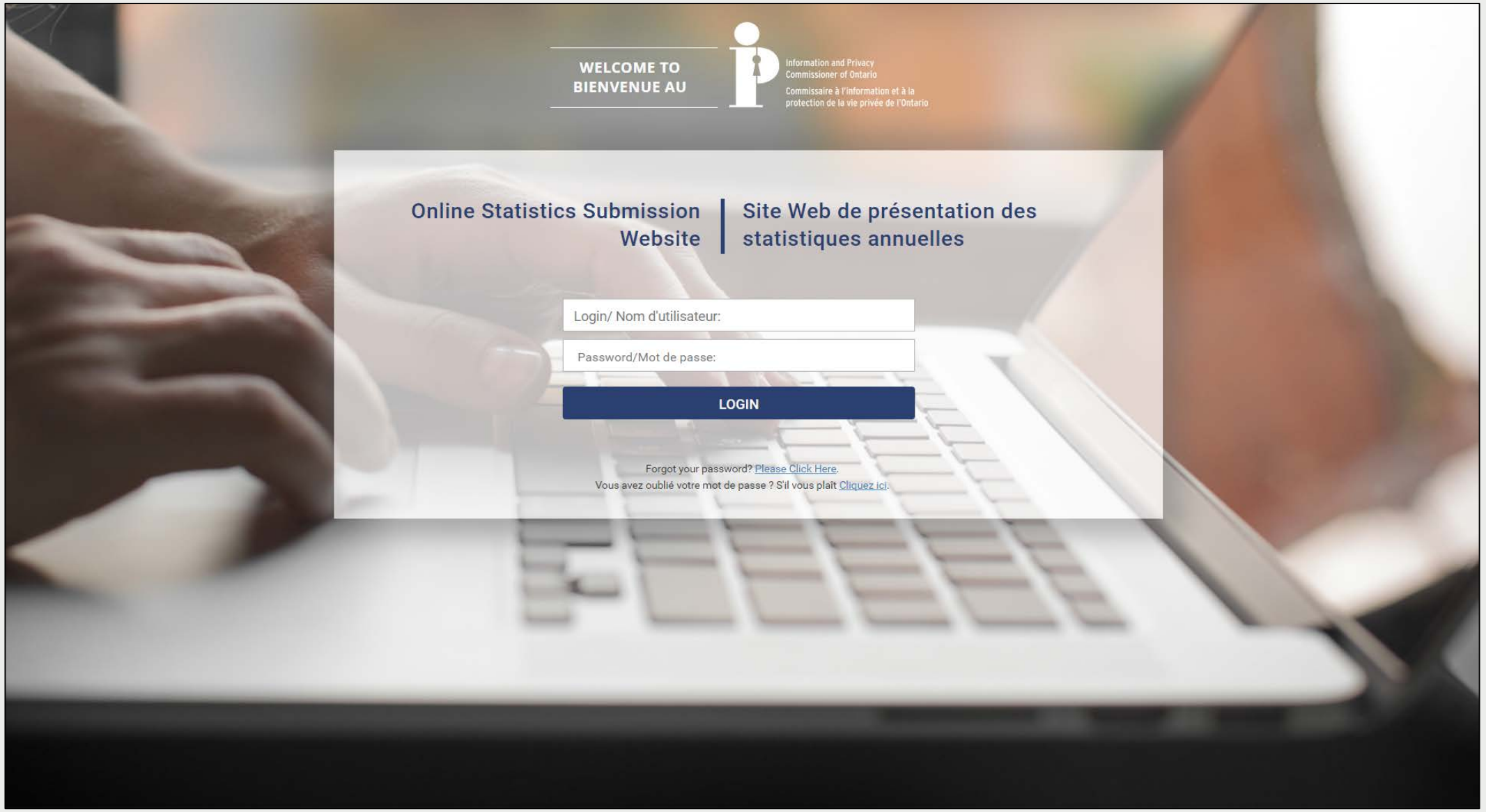
(2) The report shall be transmitted to the Commissioner by the electronic means and format determined by the Commissioner.

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.

Workbook/ Completion Guide

- The IPC has also released a Workbook and Guide on how to complete the annual report

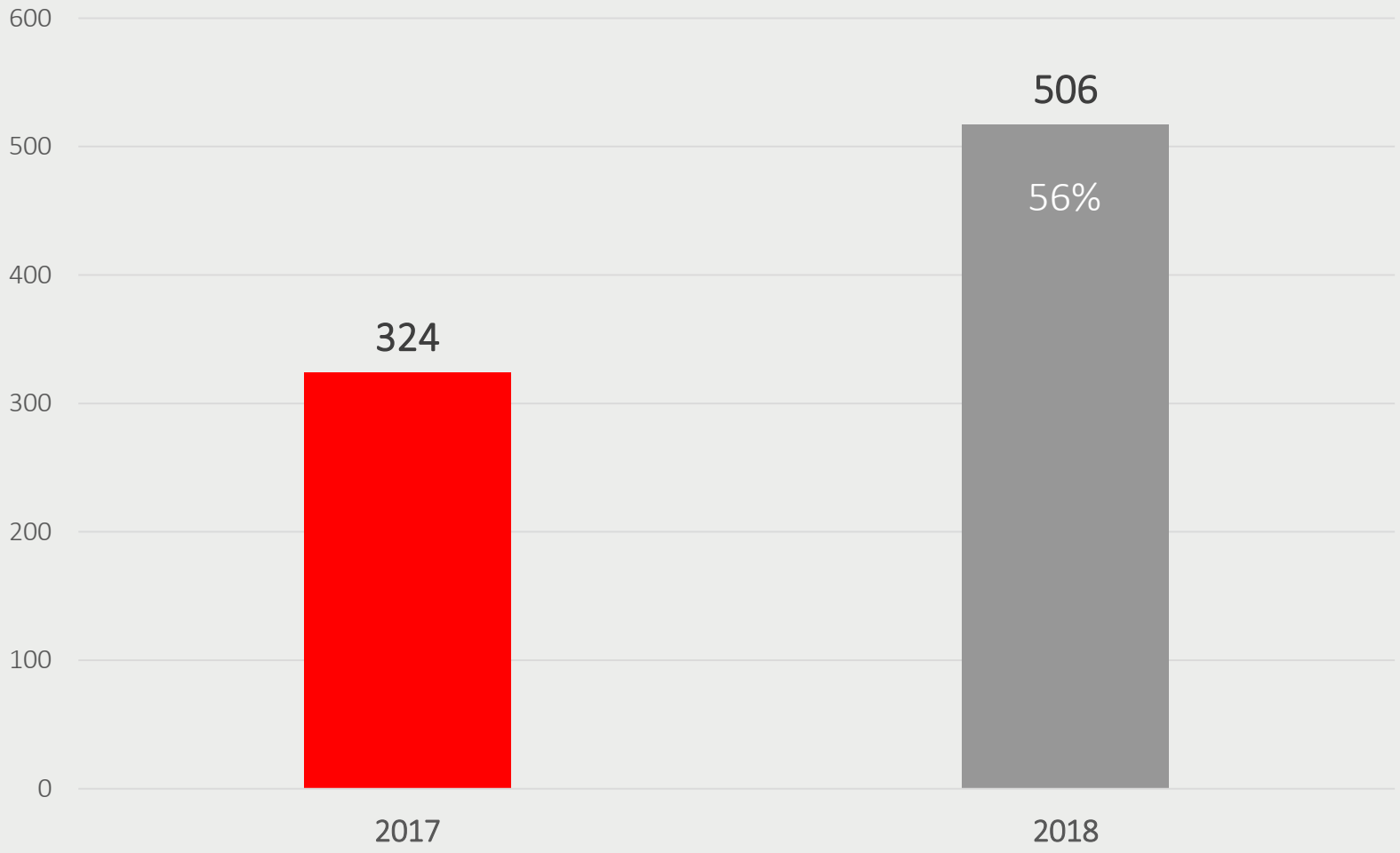



WELCOME TO
BIENVENUE AU
Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario
Online Statistics Submission Website
Site Web de présentation des statistiques annuelles
Login/ Nom d'utilisateur:
Password/Mot de passe:
LOGIN
Forgot your password? Please Click Here.
Vous avez oublié votre mot de passe ? S'il vous plaît Cliquez ici.

IPC Webinar

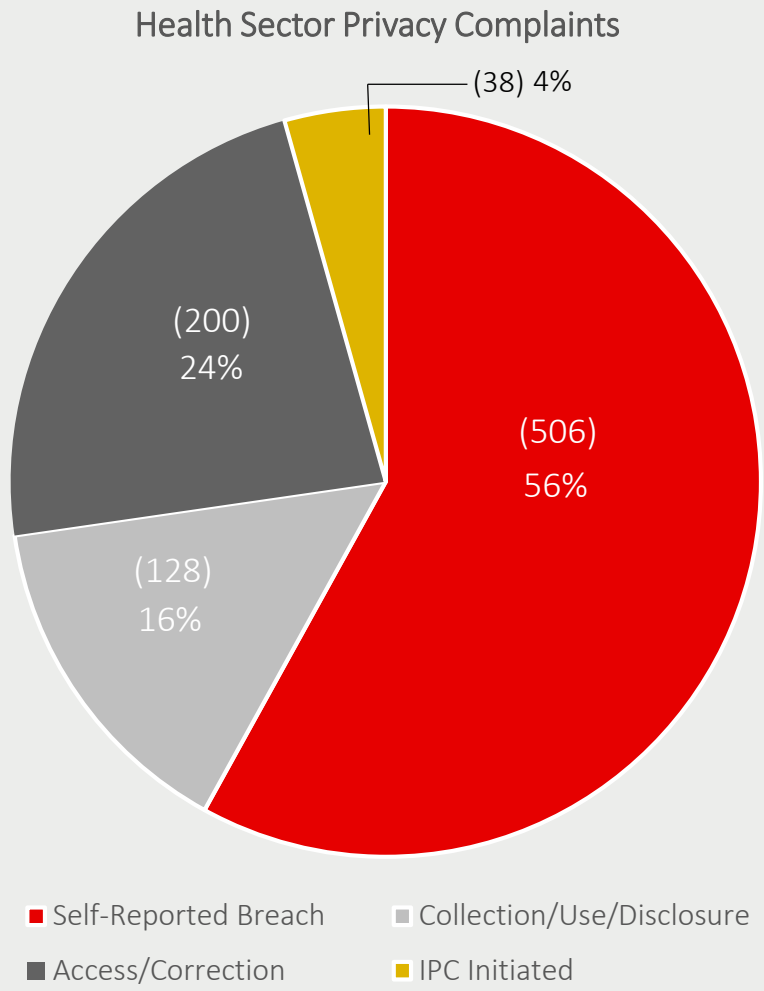
https://youtu.be/KjitJ74wn4A

Self-Reported Breaches
Before and After Mandatory Breach Reporting



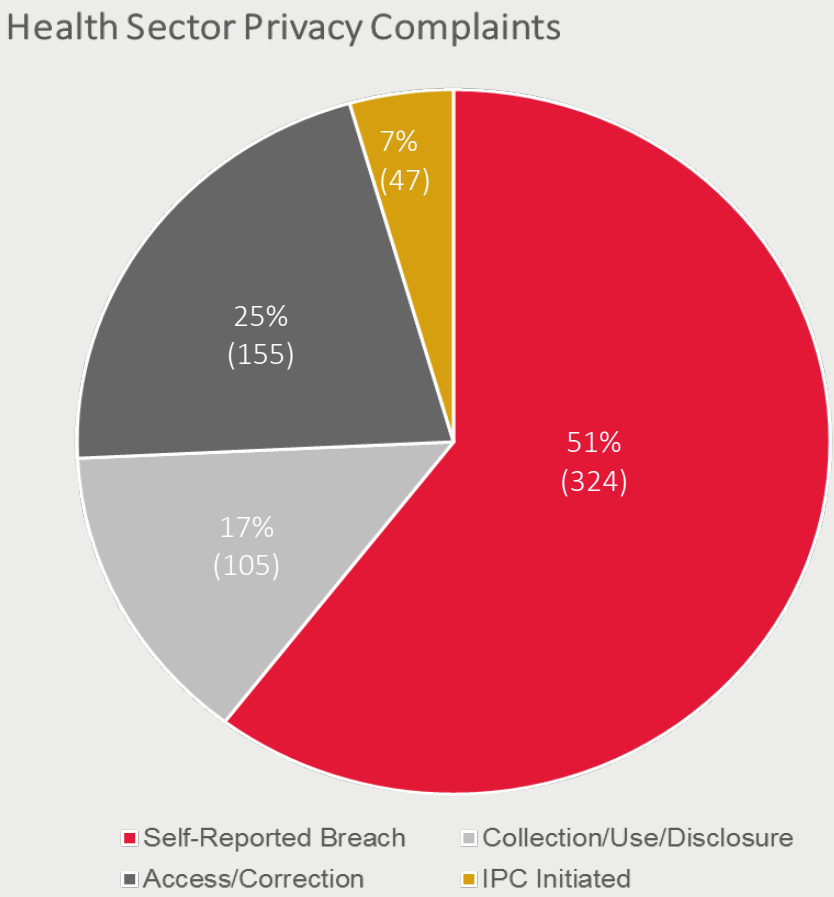
Health Sector Privacy Complaints 2018

- Of the 506 self-reported breaches in 2018:
  - 120 were snooping incidents
  - 15 were ransomware/cyberattack
- Remaining 371 were related to:
  - lost or stolen PHI
  - misdirected information
  - records not properly secured
  - other collection, use and disclosure issues

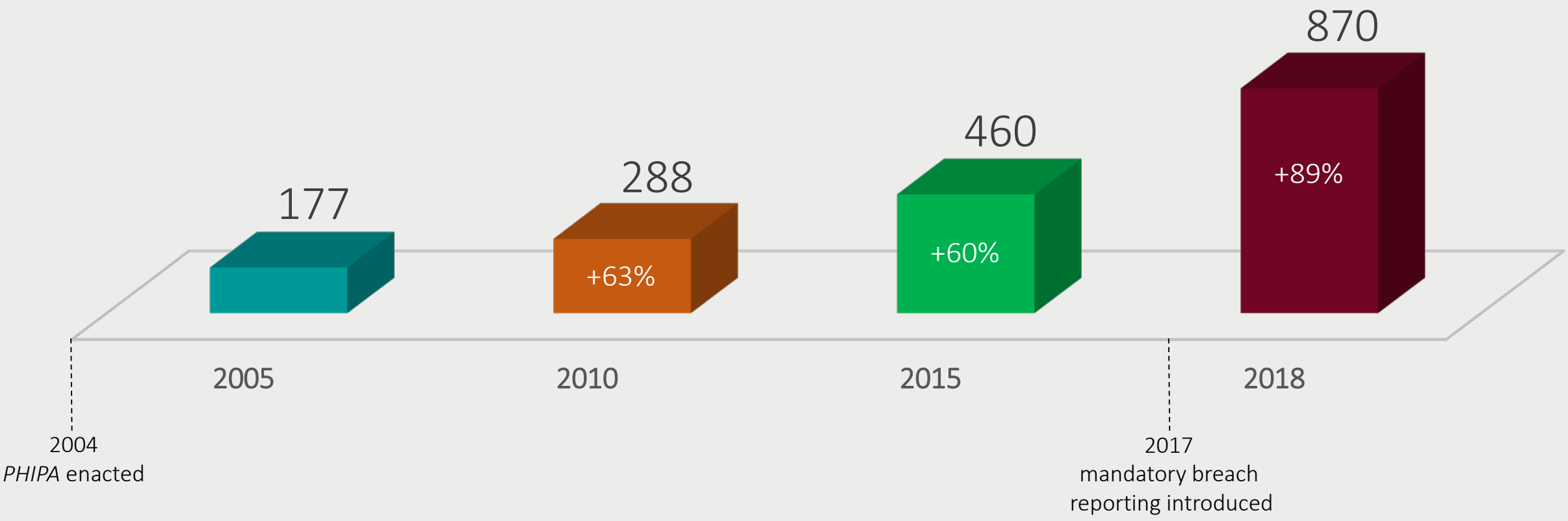


Health Sector Privacy Complaints 2017

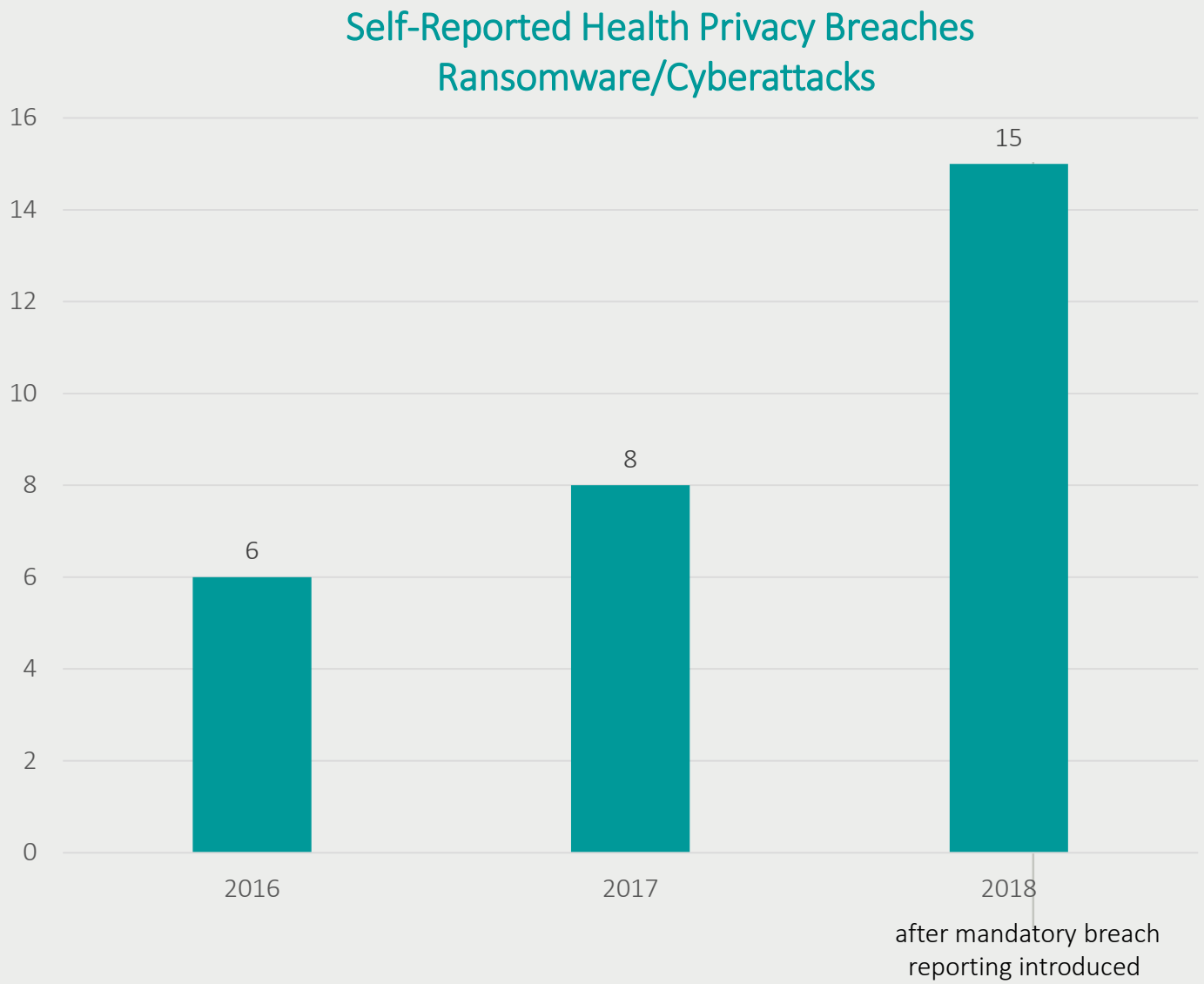
- Of the 324 self-reported breaches in 2017:
  - 60 were snooping incidents
  - 8 were ransomware/cyberattack
- Remaining 256 were related to:
  - lost or stolen PHI
  - misdirected information
  - records not properly secured
  - other collection, use and disclosure issues



Complaints Opened per Year



Cyberattacks and Ransomware



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

Technology Fact Sheet

Protecting Against Ransomware

July 2016

Ransomware has become an increasingly common and dangerous threat to the security of electronic records. This fact sheet provides information on how public institutions and healthcare organizations in Ontario can protect themselves against it.

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software, or "malware," that encrypts files on your device or computer, including any mapped or network drives, and then demands payment in exchange for the key needed to decrypt the files. It essentially locks you out of your data and holds the means of regaining access for ransom.

HOW DO COMPUTERS GET INFECTED?

Hackers use different techniques to install ransomware on computers. In general, these fall into two categories: "phishing" attacks and software exploits.

Phishing Attacks

Phishing is a type of online attack in which a hacker sends one or more individuals an unsolicited electronic communication—email, social media post or instant messenger chat—designed to trick or deceive a recipient into revealing sensitive information or downloading malware.

In the case of ransomware, the hacker will often try to impersonate an "official" correspondence relating to a common business transaction, such as a shipping notice or invoice from a delivery company. The hacker may also try to fake an "urgent matter," such as an unpaid invoice or notice of audit. More advanced versions (also known as "spear phishing") target specific individuals or places of business.

Ransomware may be installed if the recipient opens a file attachment or clicks on a link in the body of the message.

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

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

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