Regulators' Expectations and Responses to Breaches

David Goodis

Assistant Commissioner,

Information and Privacy Commissioner of Ontario

Information and Privacy
Commissioner of Ontario

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

Privacy law In Ontario and Canada

Federal Public Sector	Ontario Public Sector	Ontario Health Sector	Private Sector
Government of Canada federal ministries, agencies, crown corporations	Government of Ontario provincial ministries, agencies, hospitals, universities, cities, police, schools	Health care individuals, organizations (hospitals, pharmacies, labs, doctors, dentists, nurses)	Private sector businesses
Privacy Act	*Freedom of Information and Protection of Privacy Act* (*FIPPA*) *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)	*Personal Health Information Protection Act* (*PHIPA*)	*Personal Information Protection and Electronic Documents Act* (*PIPEDA*)
OPC oversight	IPC/O oversight	IPC/O oversight	OPC oversight

Privacy breaches

- What is a privacy breach?
  - personal information collected, retained, used, disclosed, disposed of not in compliance with privacy law
    - cyberattack (phishing or malware attack)
    - theft (theft of portable storage device—especially not encrypted)
    - access by employee for improper purpose (snooping)
    - insecure disposal

How to prevent breaches

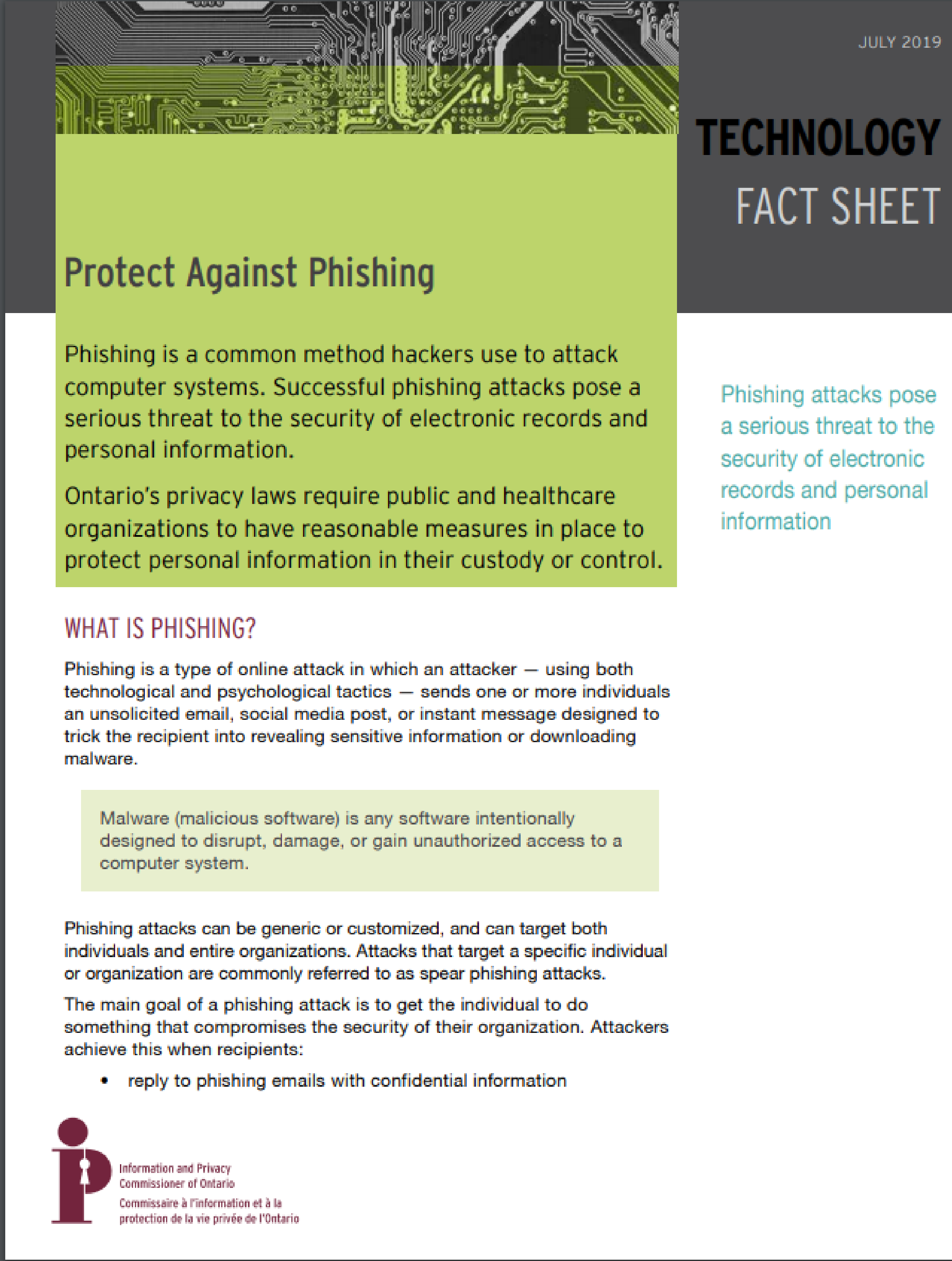
- educate employees about privacy laws, organization’s privacy policies and practices
- conduct privacy impact assessments before introducing/changing technologies, information systems to ensure privacy risks and weaknesses identified and address
- seek input from appropriate parties
  - legal counsel
  - IT security staff
  - privacy officer or coordinator
  - regulators

How to prevent breaches—safeguards

Administrative	Technical	Physical
• privacy/security policies • auditing compliance with rules • privacy and security training • data minimization • confidentiality agreements • privacy impact assessments	• strong authentication and access controls • detailed logging, auditing, monitoring • strong passwords, encryption • patch and change management • firewalls, anti-virus, anti-spam, anti-spyware • protection against malicious code • threat risk assessments, ethical hacks	• controlled access to premises • controlled access to locations within premises where PI is stored • access cards and keys • ID, screening, supervision of visitors NOTE – when determining appropriate safeguards consider • sensitivity and amount of information • number and nature of people with access to the information • threats and risks associated with the information

IPC technology fact sheet - protect against phishing

- what is a phishing attack and how do you prevent one?
- how do you respond?
- key messages for training employees



JULY 2019

TECHNOLOGY
FACT SHEET

Protect Against Phishing

Phishing is a common method hackers use to attack computer systems. Successful phishing attacks pose a serious threat to the security of electronic records and personal information.

Ontario's privacy laws require public and healthcare organizations to have reasonable measures in place to protect personal information in their custody or control.

Phishing attacks pose a serious threat to the security of electronic records and personal information

WHAT IS PHISHING?

Phishing is a type of online attack in which an attacker — using both technological and psychological tactics — sends one or more individuals an unsolicited email, social media post, or instant message designed to trick the recipient into revealing sensitive information or downloading malware.

> Malware (malicious software) is any software intentionally designed to disrupt, damage, or gain unauthorized access to a computer system.

Phishing attacks can be generic or customized, and can target both individuals and entire organizations. Attacks that target a specific individual or organization are commonly referred to as spear phishing attacks.

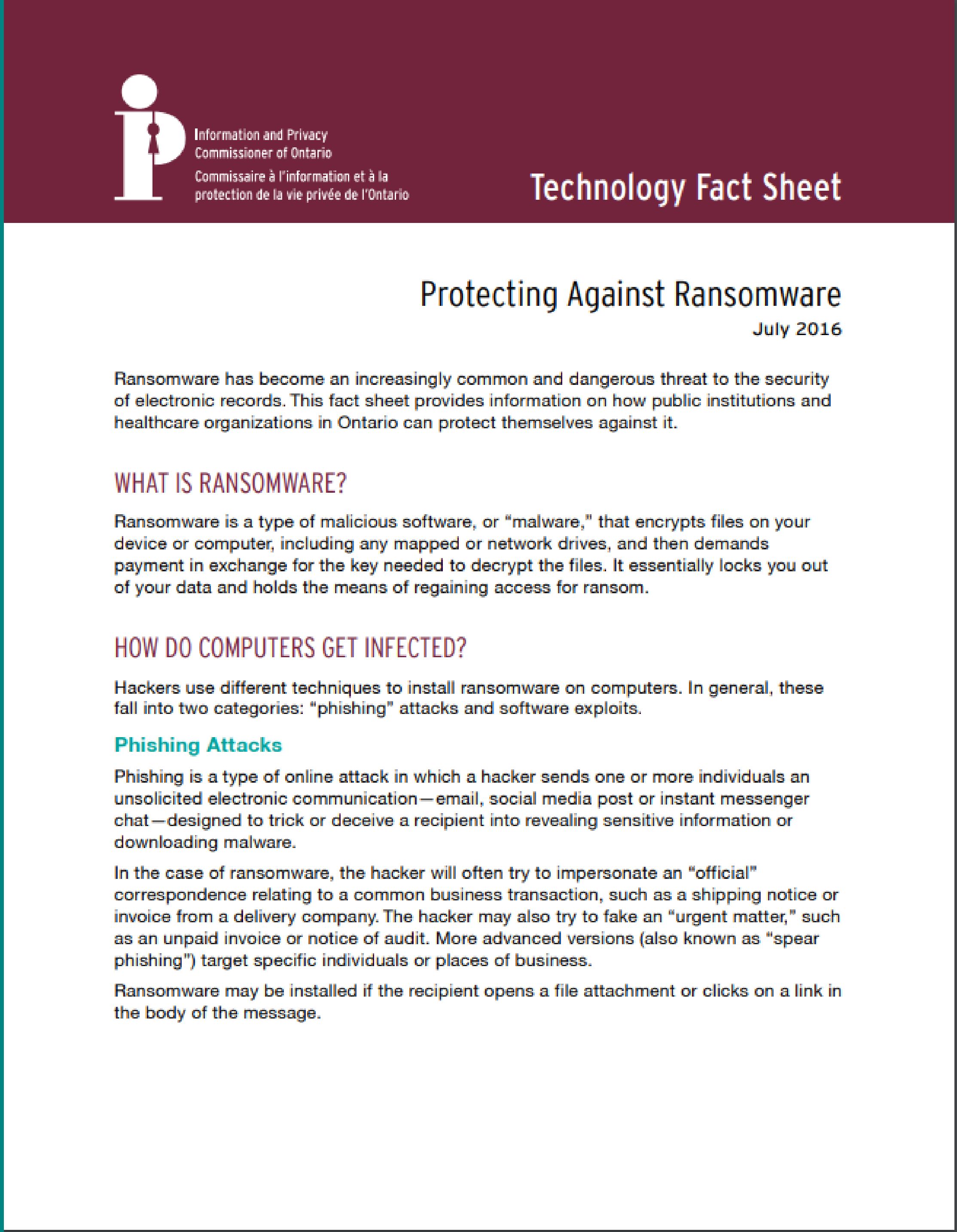
The main goal of a phishing attack is to get the individual to do something that compromises the security of their organization. Attackers achieve this when recipients:

- reply to phishing emails with confidential information

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

IPC technology fact sheet – protect against ransomware

- what is ransomware and how do you protect your organization from a ransomware attack?



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.

Responding to a privacy breach

- have breach response plan - steps to take when breach occurs
- plan will depend on organization type, nature/amount of personal information organization deals with
- plan should include steps to ensure organization complies with privacy law duties

Responding to a privacy breach

- notify affected individuals
- investigate the breach
  - identify, analyze events that led to breach, determine cause
  - if breach due to systemic issue, review program-wide procedures
  - review breach response plans, privacy policies, staff training
- notify Commissioner
  - can provide quick advice
  - early notification may enhance reputation, put you in better position with regulator, possibly help with future litigation

Responding to a privacy breach

- corrective action to prevent similar breaches
  - educate staff about privacy law and organization's personal information policies
  - conduct privacy impact assessment (PIA) before introducing or changing technologies, information systems
  - seek input from appropriate parties such as legal counsel, security units, privacy officer, Commissioner

What happens when IPC investigates?

- Commissioner may
  - assess if breach contained
  - determine if affected individuals notified
  - interview individuals involved
  - review, advise on organization's policies and procedures
  - issue a report with recommendations (or order if health info)
- investigation forward looking – how to prevent future breaches?

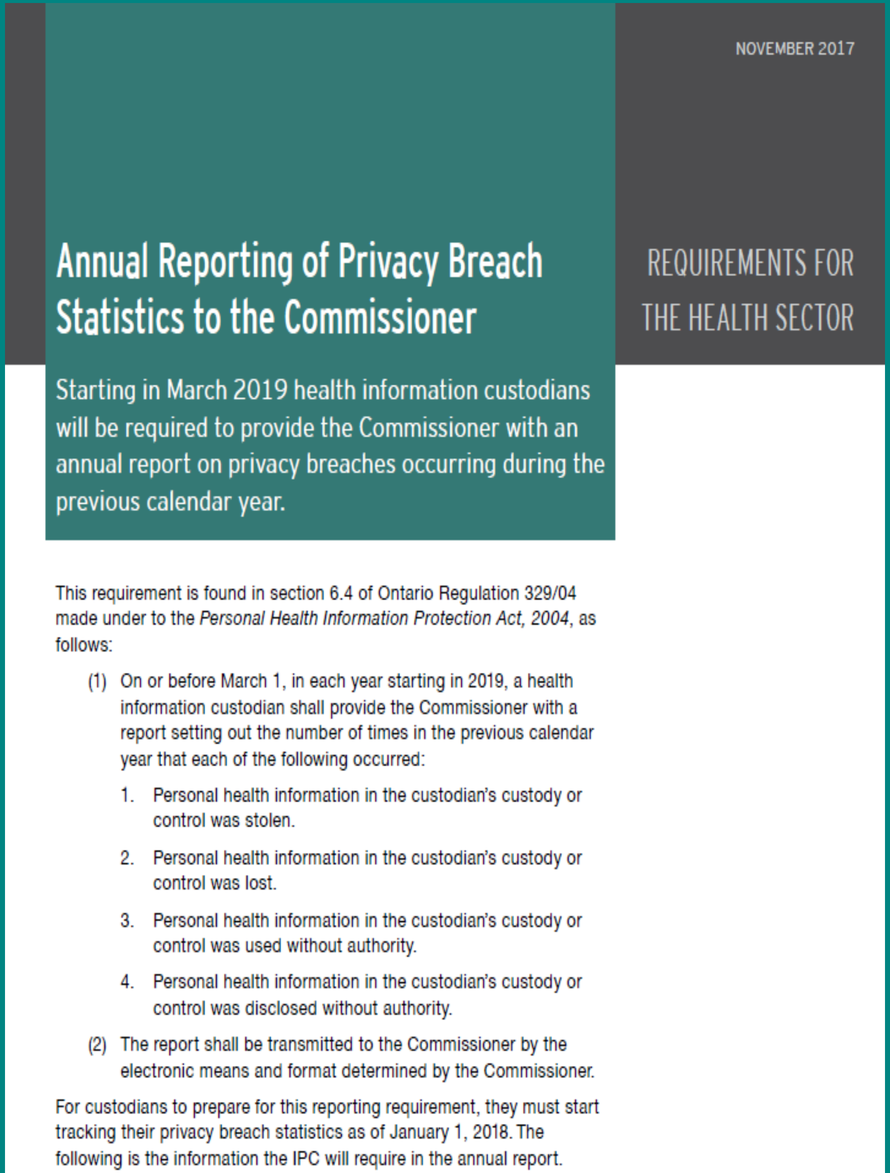
Reporting and notification

- organizations experiencing breach must consider whether they should (*M/FIPPA*) or must (*PHIPA*):
  - notify affected individuals
  - report breach to regulator

PHIPA reporting obligations

- affected individuals
  - HIC must notify affected individual at first reasonable opportunity if PHI stolen, lost, used/disclosed without authority
- IPC
  - HIC must notify IPC if circumstances surrounding theft, loss, unauthorized use/disclosure meet prescribed requirements

PHIPA Breach Reporting Guidance Documents



NOVEMBER 2017

REQUIREMENTS FOR THE HEALTH SECTOR

Annual Reporting of Privacy Breach Statistics to the Commissioner

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.

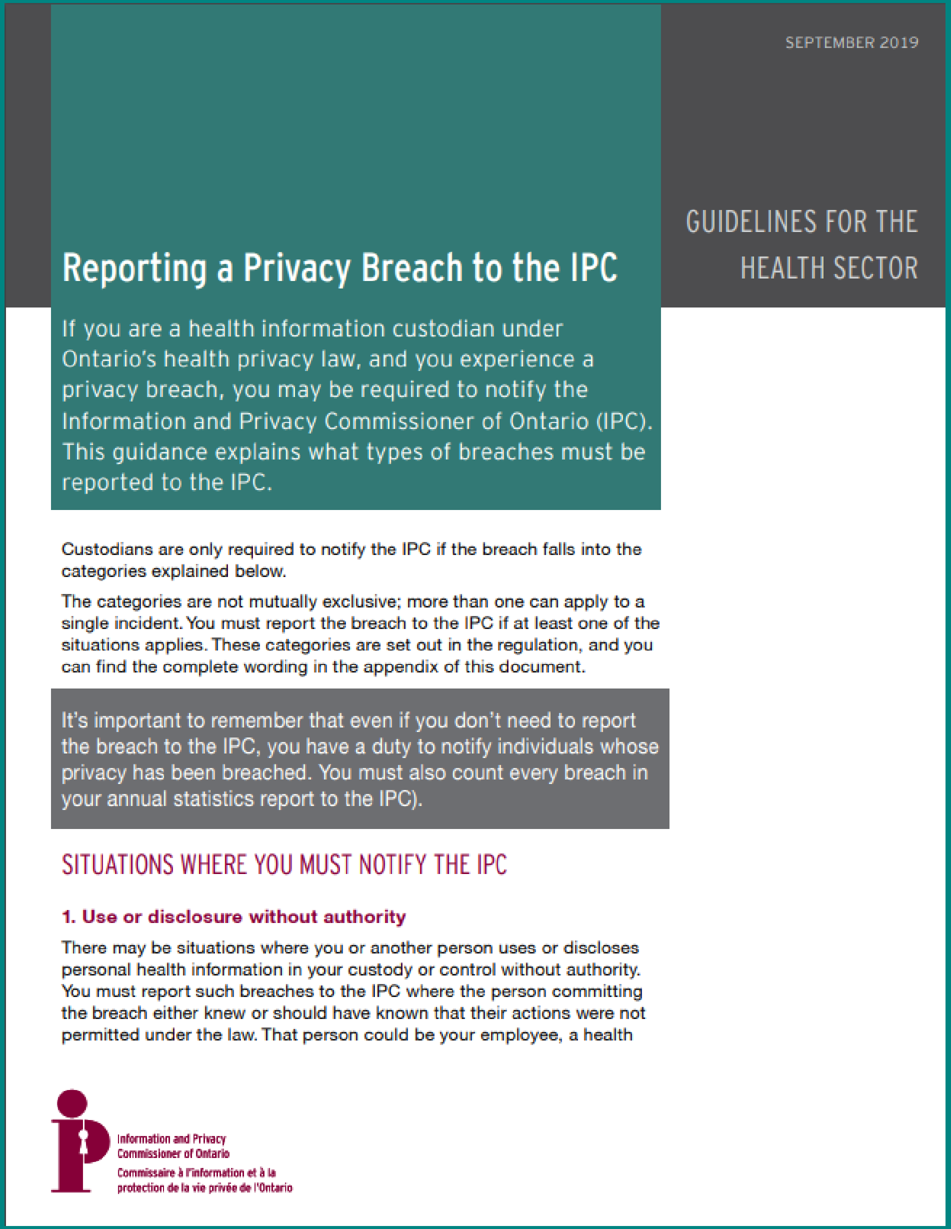
This requirement is found in section 6.4 of Ontario Regulation 329/04 made under to the *Personal Health Information Protection Act, 2004*, as follows:

(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.



SEPTEMBER 2019

GUIDELINES FOR THE HEALTH SECTOR

Reporting a Privacy Breach to the IPC

If you are a health information custodian under Ontario's health privacy law, and you experience a privacy breach, you may be required to notify the Information and Privacy Commissioner of Ontario (IPC). This guidance explains what types of breaches must be reported to the IPC.

Custodians are only required to notify the IPC if the breach falls into the categories explained below.

The categories are not mutually exclusive; more than one can apply to a single incident. You must report the breach to the IPC if at least one of the situations applies. These categories are set out in the regulation, and you can find the complete wording in the appendix of this document.

It's important to remember that even if you don't need to report the breach to the IPC, you have a duty to notify individuals whose privacy has been breached. You must also count every breach in your annual statistics report to the IPC).

SITUATIONS WHERE YOU MUST NOTIFY THE IPC

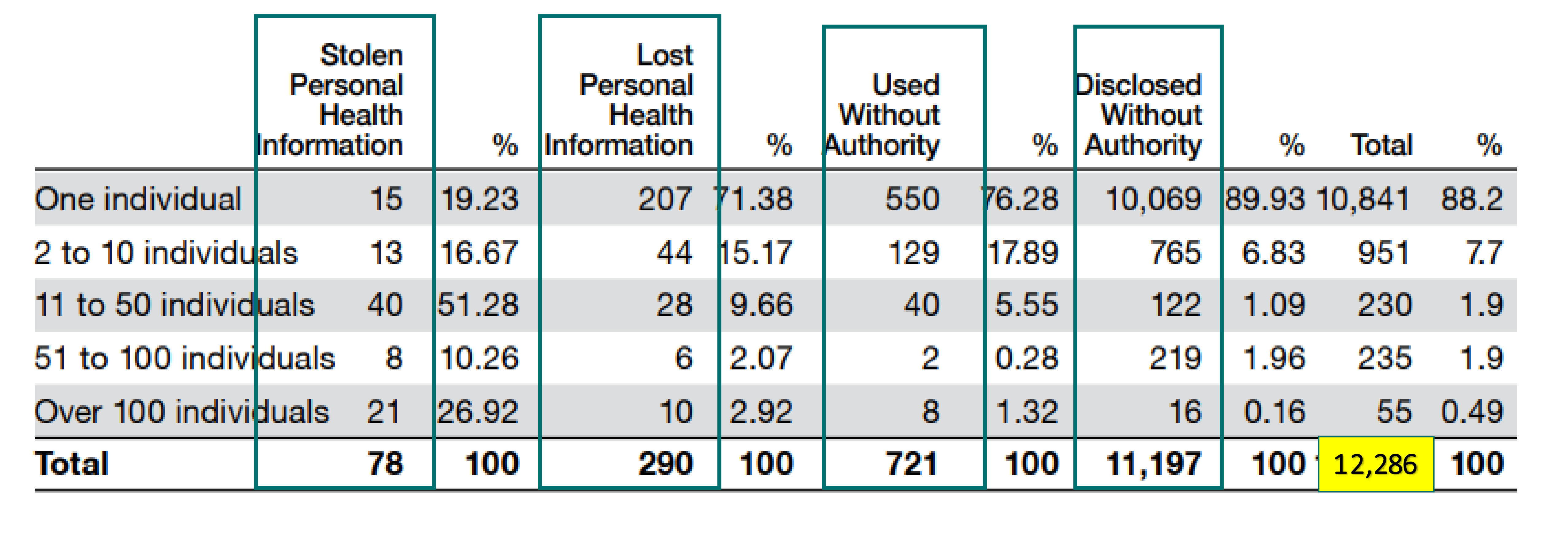
1. Use or disclosure without authority

There may be situations where you or another person uses or discloses personal health information in your custody or control without authority. You must report such breaches to the IPC where the person committing the breach either knew or should have known that their actions were not permitted under the law. That person could be your employee, a health

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

PHIPA reported privacy breaches

- 12,286 reported to IPC in 2019



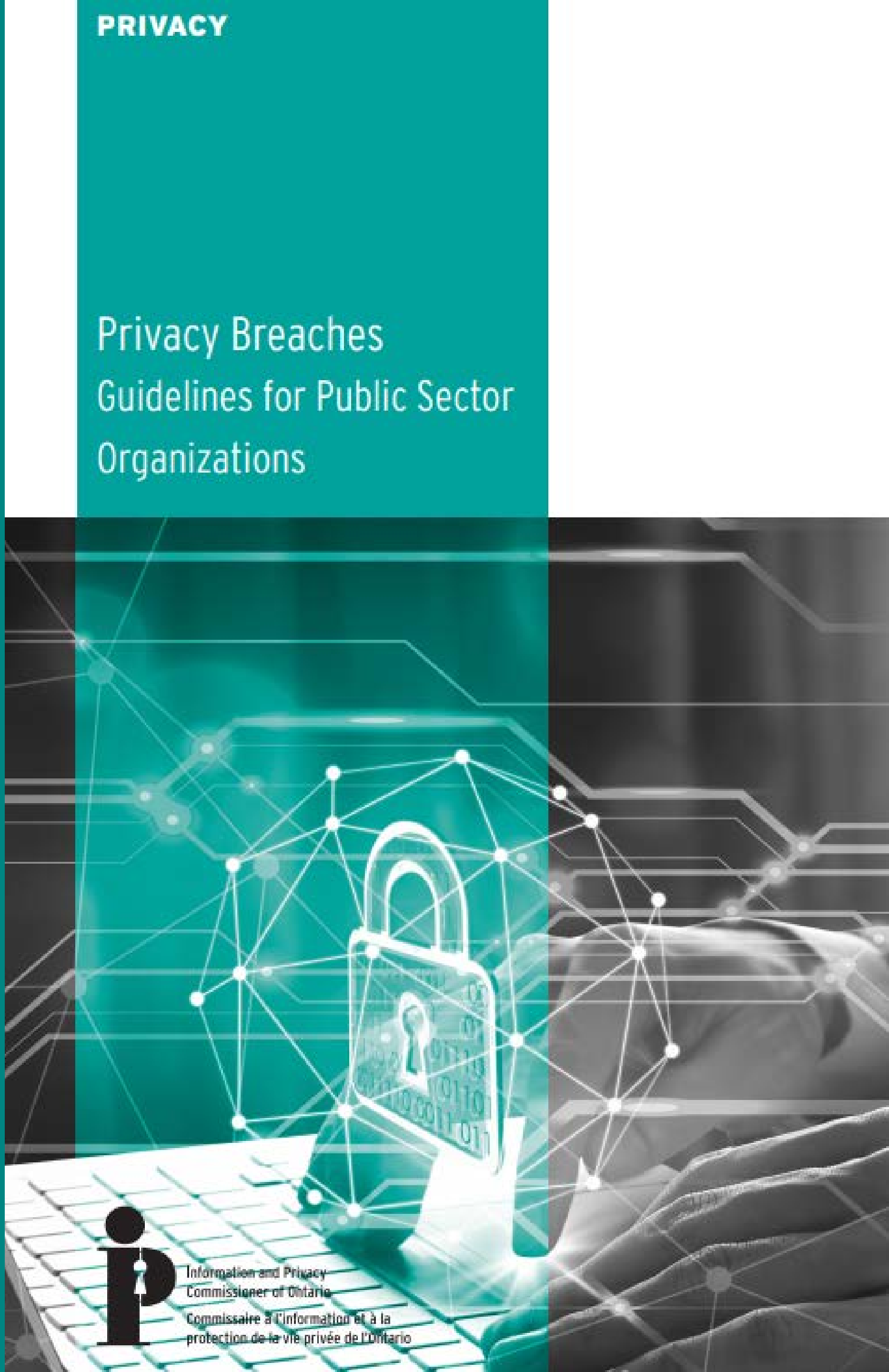
	Stolen Personal Health Information	%	Lost Personal Health Information	%	Used Without Authority	%	Disclosed Without Authority	%	Total	%
One individual	15	19.23	207	71.38	550	76.28	10,069	89.93	10,841	88.2
2 to 10 individuals	13	16.67	44	15.17	129	17.89	765	6.83	951	7.7
11 to 50 individuals	40	51.28	28	9.66	40	5.55	122	1.09	230	1.9
51 to 100 individuals	8	10.26	6	2.07	2	0.28	219	1.96	235	1.9
Over 100 individuals	21	26.92	10	2.92	8	1.32	16	0.16	55	0.49
Total	**78**	**100**	**290**	**100**	**721**	**100**	**11,197**	**100**	12,286	**100**

FIPPA/MFIPPA

- no legislated requirement to report breaches to IPC
- institutions should notify IPC of significant breaches such as those involving sensitive PI, or large number of individuals, where institution having trouble containing breach, or where breach unusual/unique
- notify IPC as soon as reasonably possible
- notify IPC before notifying affected individuals so IPC is prepared to respond to inquires

IPC guidance: privacy breaches - guidelines for public sector organizations

- obligations, best practices for public sector organizations experiencing data breaches



PRIVACY

Privacy Breaches
Guidelines for Public Sector Organizations

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

Cooperation between regulators

- privacy regulators in Canada and internationally may cooperate to address multi-jurisdictional issues:
  - Casino Rama cyber attack (2016)
    - IPC/O oversees Ontario Lottery and Gaming Corporation (*FIPPA* public institution)
    - Privacy Commissioner of Canada oversees Casino Rama operator (private sector company)
  - Global Privacy Enforcement Network Sweeps—global privacy regulators examine privacy implications of a particular type of product or service (e.g. health devices, educational apps)

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