REACHING OUT TO ONTARIO

PROTECTING PERSONAL HEALTH INFORMATION

Debra Grant
Director of Health Policy

Suzanne Brocklehurst
Registrar

REACHING OUT TO ONTARIO

HAMILTON

May 11, 2018

Topics

1. Email communications
2. Abandoned records
3. Unauthorized access
4. Point-in-time breach reporting
5. Annual breach reporting

EMAIL 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 by Email

- The *Personal Health Information Protection Act* (*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

ABANDONED RECORDS

Abandoned Records

- Since *PHIPA* came into effect, the IPC has investigated numerous instances of abandoned health records
- This typically occurs when a custodian relocates, retires, becomes incapacitated or otherwise ceases to practice
- Despite the legislative requirements to safeguard PHI in the custody or control of a custodian, records of PHI continue to be abandoned
- No entity or person has the authority to assume custody and control of abandoned records
- This may lead to privacy breaches, patients not being able to exercise their right of access, and health care providers not have accurate and complete information for health care purposes

Previous Guidance

- In 2007, the IPC issued guidance on how to avoid abandoned records
  - *How to Avoid Abandoned Records: Guidelines on the Treatment of Personal Health Information, in the Event of a Change in Practice*
  - *Checklist for Health Information Custodians in the Event of a Planned or Unforeseen Change in Practice*
- The guidance focused on what to do in the event of a change in practice

How to Avoid Abandoned Records

- Who is the custodian in the event of a change in practice?
- What obligations are imposed on custodians in the event of a change in practice?
- What are best practices in the event of a change in practice?

Information and Privacy Commissioner/ Ontario

How to Avoid Abandoned Records: Guidelines on the Treatment of Personal Health Information, in the Event of a Change in Practice

Ongoing Challenges

- Custodians are not being proactive, and records are being left behind or disposed of in an unsecure manner
- It may be difficult to identify or locate the custodian
- There may be no plan for transferring custody and control if the practitioner becomes incapacitated or dies
- There may be no plan for ongoing retention of records when a practitioner retires or relocates to another jurisdiction

Jurisdictional Scan – Codes of Conduct

- Some regulatory colleges have included the requirement for members to notify the college before they leave or move their practice in their policies and codes of conduct
- Notification must include the location and disposition of records and a named successor who will provide continued access to the records
- Some regulatory colleges have made the abandonment of health records an act of professional misconduct

Jurisdictional Scan – Amendments to Health Privacy Law

- Some jurisdictions supplemented the initiatives of regulatory colleges with amendments to their health privacy legislation
- Saskatchewan amended its *Health Information Protection Act* to authorize the Ministry of Health to appoint a person to act in place of a former trustee who abandoned records
- Additionally, abandoning records in Saskatchewan is now subject to a liability offence of up to $50,000 for individuals
- Saskatchewan includes a reverse onus clause – this means trustees must demonstrate that they took reasonable steps to prevent the abandonment of the records

Jurisdictional Scan – Amendments to Laws Governing Providers

- Some jurisdictions supplemented the initiatives of regulatory colleges with amendments to legislation governing providers
- Manitoba amended its *Regulated Health Professions Act*
- This amendment has not yet been proclaimed
- When proclaimed, the College will be permitted to appoint a member to take over the responsibility of securing the records or apply to the Court to designate a custodian
- Members of each college will have a duty to ensure that their records are not abandoned
- Members who abandon health records will be guilty of an offence and liable to a fine up to $50,000

Potential Solutions

- Policy Solutions
  - education and awareness
  - amendments to regulatory colleges policies and procedures
  - amendments to professional codes of conduct
- Legislative Solutions
  - amendments to health privacy legislation
  - amendments to legislation governing health professionals

UNAUTHORIZED ACCESS

Meaning of Unauthorized Access

- When you view, handle or otherwise deal with PHI without consent and for purposes not permitted by *PHIPA*, for example:
  - when not providing or assisting in the provision of health care to the individual
  - when not necessary for the purposes of exercising employment, contractual or other responsibilities
- The act of viewing PHI on its own, without any further action, is an unauthorized access

Examples of Unauthorized Access – Education and Quality Improvement

- There have been a number of instances where agents have accessed PHI claiming it was for:
  - their own educational purposes
  - to improve the quality of the health care they provide
  - other uses permitted by *PHIPA*
- 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 what access is permitted and is not permitted, including through training, notices, flags, agreements, etc.

Examples of Unauthorized Access – Health Professionals with Privileges

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

Health Professionals with Privileges

- The roles of the hospital, doctor and doctor's staff should be specified, in a written agreement, to clarify who is:
  - a custodian
  - an agent of the hospital
  - an agent of the health professional
- The agreement should also clarify who is responsible for ensuring there is appropriate training, that confidentiality agreements are signed, that policies and procedures are followed, etc.

Consequences of Unauthorized Access

- Review or investigation by privacy oversight bodies
- Prosecution for offences
- Statutory or common law actions
- Discipline by employers
- Discipline by regulatory bodies

Orders HO-002, HO-010 and HO-013

- Our office has issued three orders involving unauthorized access:
- **Order HO-002**
  - A registered nurse accessed records of the estranged spouse of her boyfriend to whom she was not providing care
  - They were accessed over six-weeks during divorce proceedings
- **Order HO-010**
  - A diagnostic imaging technologist accessed records of the current spouse of her former spouse to whom she was not providing care
  - They were accessed on six occasions over nine months
- **Order HO-013**
  - Two employees accessed records to market and sell RESPs

Offences

- It is an offence to wilfully collect, use or disclose PHI in contravention of *PHIPA*
- Consent of the Attorney General is required to commence a prosecution for offences under *PHIPA*
- On conviction, an individual may be liable to a fine of up to $100,000 and a corporation of up to $500,000

Prosecutions

To date, six individuals have been prosecuted:

- **2011** – A nurse at North Bay Health Centre
- **2016** – Two radiation therapists at a Toronto Hospital
- **2016** – A registration clerk at a regional hospital
- **2017** – A social worker at a family health team
- **2017** – An administrative support clerk at a Toronto hospital

How to Reduce the Risk...

- Clearly articulate the purposes for which employees, staff and other agents may access PHI
- 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 PHI
- Impose appropriate discipline for unauthorized access

Detecting and Deterring Unauthorized Access

- 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

Detecting and Deterring Unauthorized Access to Personal Health Information

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

BREACH REPORTING

Breach Reporting

Section 6.3 of *Ontario Regulation* 329/04 states a health information 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

Breach Notification to the IPC

- The IPC has published a guidance document providing more detail about when a breach must be reported

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

Use or Disclosure Without Authority

The health information custodian has reasonable grounds to believe that personal health information in the custodian's 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.

- Custodians must notify the IPC where there are reasonable grounds to believe the person committing the breach knew or ought to have known their use or disclosure was not permitted by the custodian or *PHIPA*
- Example: A nurse looks at his or her neighbour's medical record for no work- related purpose

Stolen Information

The health information custodian has reasonable grounds to believe that personal health information in the custodian's custody or control was stolen.

- Custodians must notify the IPC of the theft of paper or electronic records containing personal health information
- Example: Theft of a laptop computer containing identifying personal health information that was not encrypted or properly encrypted

Further Use or Disclosure Without Authority After Breach

The health information custodian has reasonable grounds to believe that, after an initial loss or unauthorized use or disclosure of personal health information in the custodian's custody or control, the personal health information was or will be further used or disclosed without authority.

- Custodians must notify the IPC where there are reasonable grounds to believe that the personal health information subject to the breach was or will be further used or disclosed without authority (e.g. to market products or services, for fraud, to gain a competitive advantage in a proceeding, etc.)
- Example: A custodian inadvertently sends a fax containing patient information to the wrong recipient and although the recipient returned the fax, the custodian becomes aware that he or she kept a copy and is threatening to make it public

Pattern of Similar Breaches

The loss or unauthorized use or disclosure of personal health information is part of a pattern of similar losses or unauthorized uses or disclosures of personal health information in the custody or control of the health information custodian.

- The pattern may indicate systemic issues that need to be addressed
- Example: A letter to a patient inadvertently included information of another patient. The same mistake re-occurs several times in the course of a couple months as a result of a new automated process for generating letters

Disciplinary Action Against a College Member

The health information custodian is required to give notice to a College of an event described in section 17.1 of *PHIPA* that relates to a loss or unauthorized use or disclosure of personal health information.

- The purpose of this section is to require the IPC to be notified of losses or unauthorized uses and disclosures in the same circumstances a custodian is required to notify a college under section 17.1 of *PHIPA*
- Example: A hospital suspends the privileges of a doctor for accessing the personal health information of his or her ex-spouse for no work-related purpose. The hospital must report this to the College of Physicians and Surgeons of Ontario and to the IPC.

Disciplinary Action Against a Non-College Member

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 *PHIPA* that relates to a loss or unauthorized use or disclosure of personal health information.

- Recognizes that not all agents of a custodian are members of a College
- The purpose of this section is to require custodians to notify the IPC of losses or unauthorized uses and disclosures in the same circumstances that a custodian is required to notify a college under section 17.1 of *PHIPA*
- Example: A hospital registration clerk posts information about a patient on social media and the hospital suspends the clerk. The clerk does not belong to a regulated health professional college.

Significant Breach

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.

Significant Breach

- To determine if a breach is significant, consider all relevant circumstances, including whether:
  - the information is sensitive
  - the breach involves a large volume of information
  - the breach involves many individuals' information
  - more than one custodian or agent was responsible for the breach
- Example: Disclosing mental health information of a patient to a large email distribution group rather than just to the patient's healthcare practitioner

Statistics

	October 1, 2017-December 31, 2017	October 1, 2016-December 31, 2016
Total Breaches	125	58
Misdirected/Lost	36.7%	28%
Snooping	24%	24%
Unauthorized collection, use, disclosure	18.4%	15%
Stolen/Inadequately secured	20.9%	33%

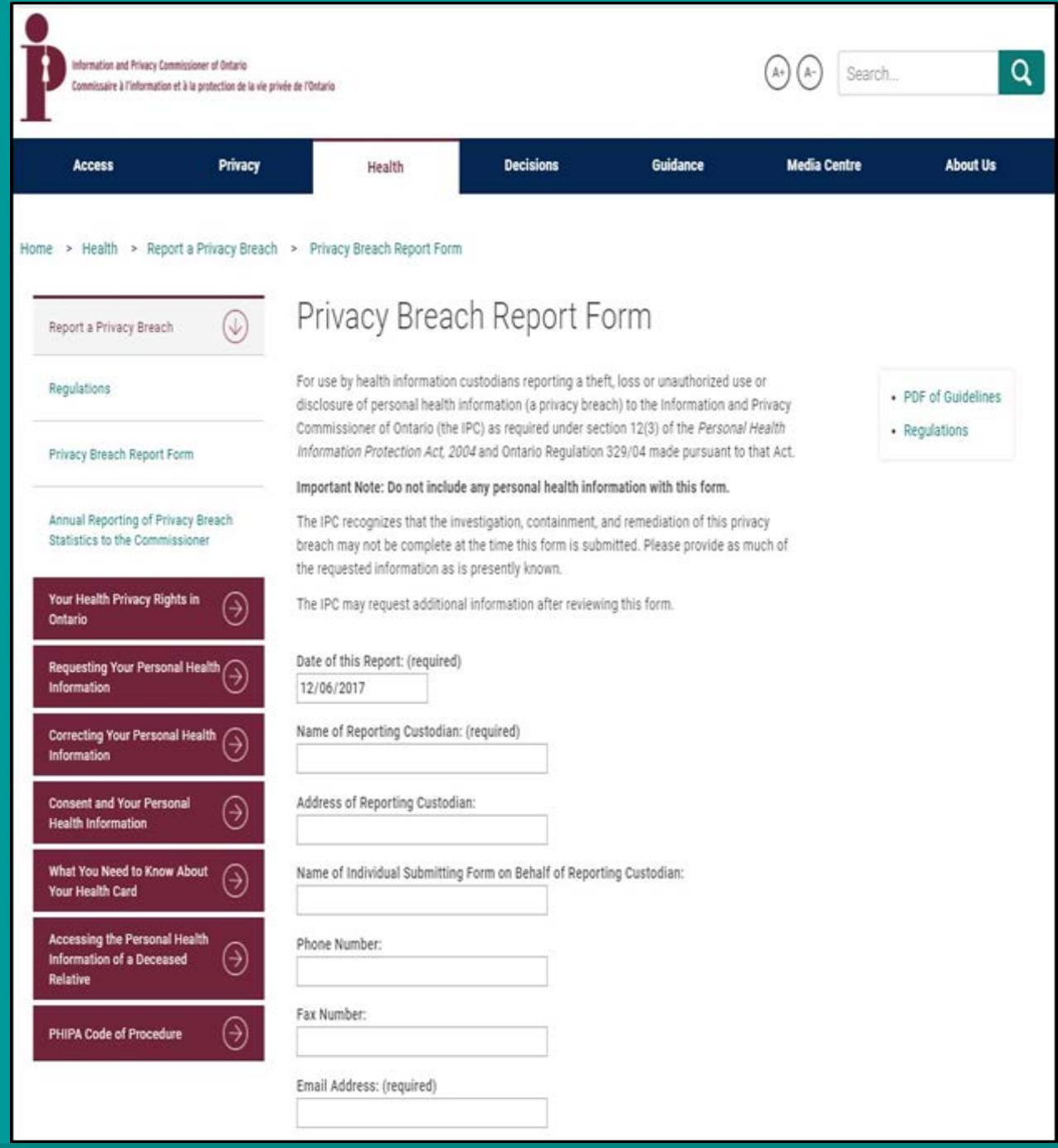
- The total number of breaches reported between October 1, 2017-December 31, 2017 represents a 115% increase over the same period in the previous year.

IPC Privacy Breach Online Report Form

Although you can report breaches by mail or fax, we recommend that you use our online report form

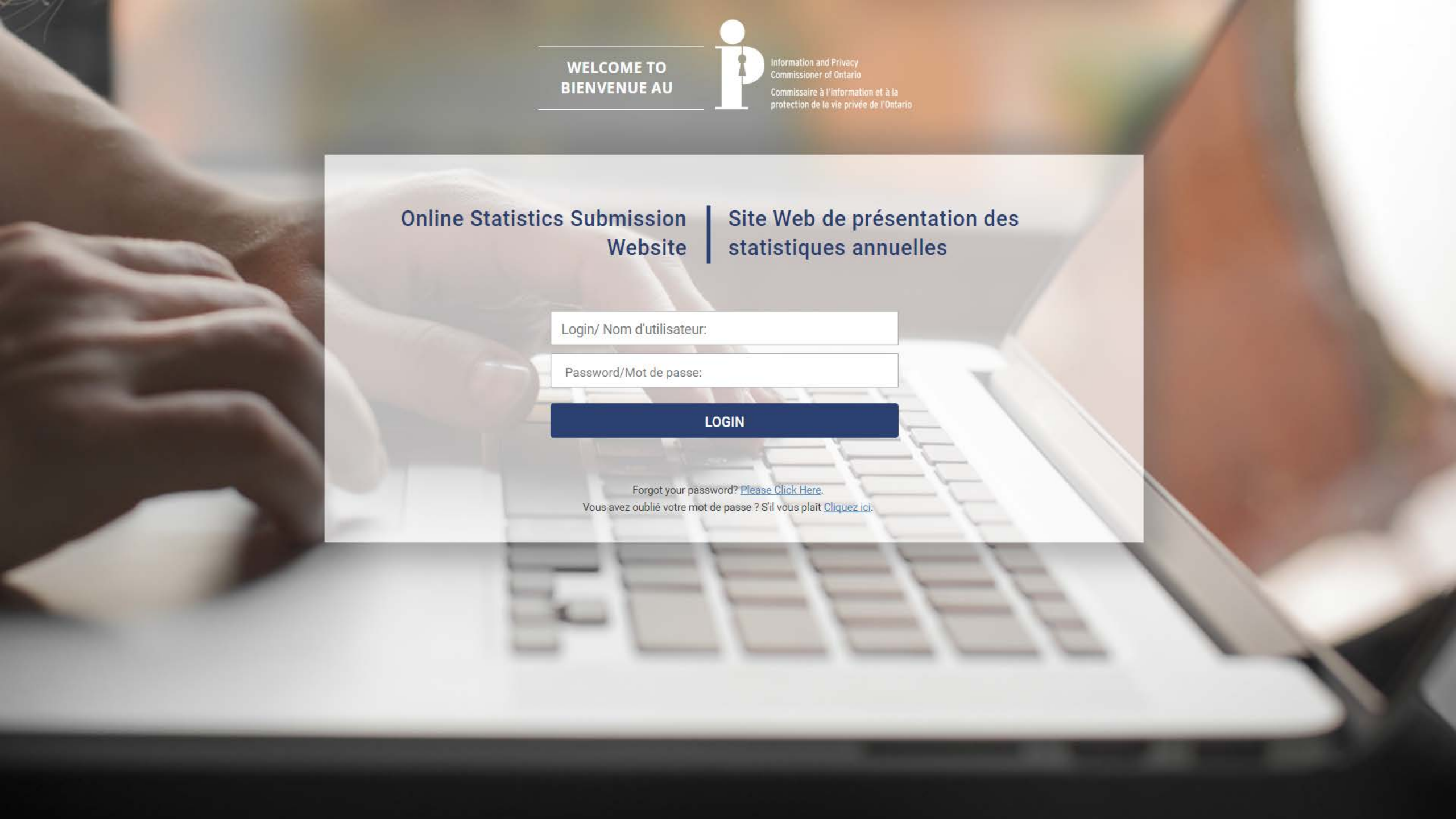
You will be asked to provide:

- 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



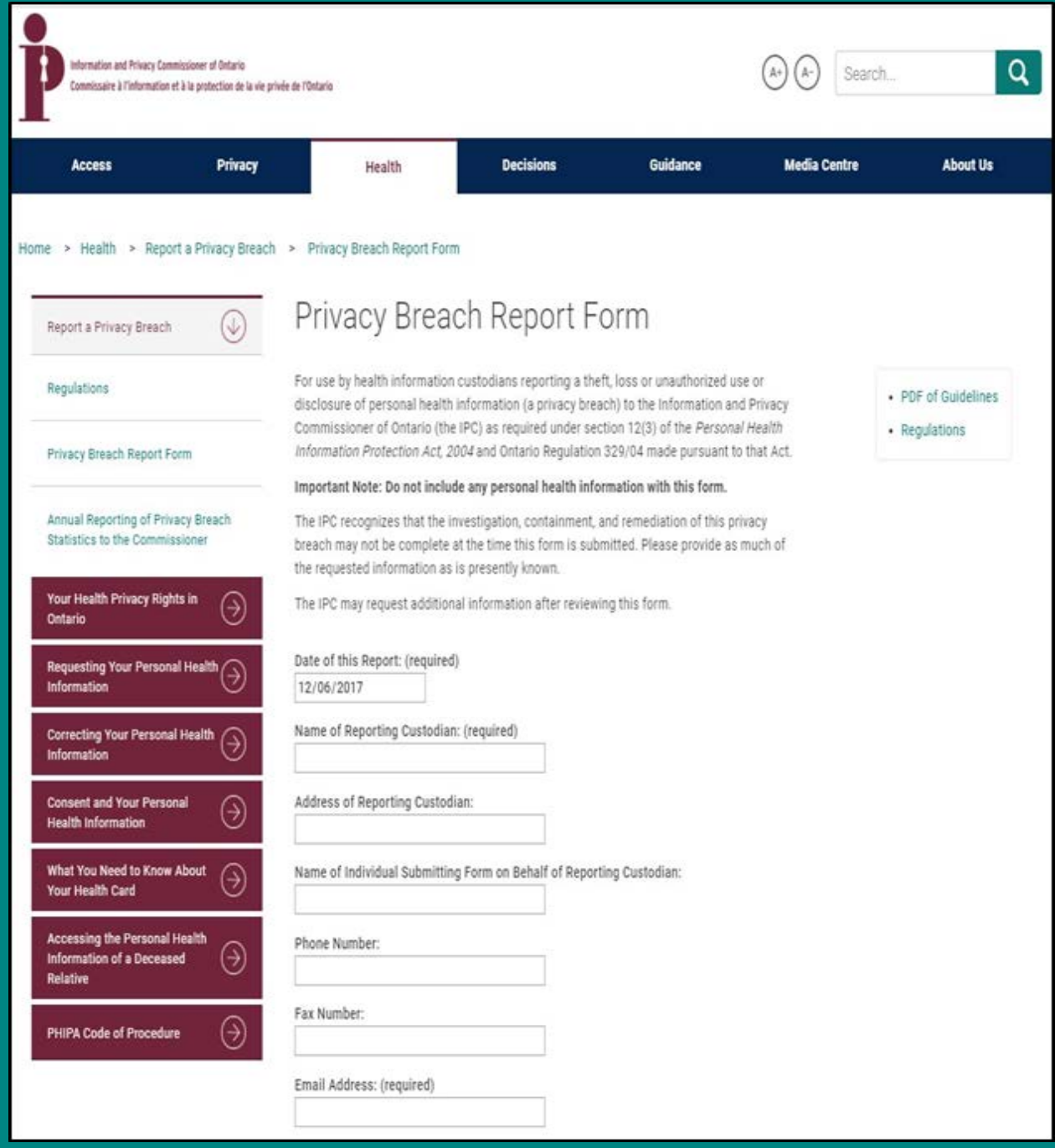
You reported a breach to the IPC, what happens next?

- A notice will be sent that reflects the type of breach reported
- A response to the notice will be requested
- Additional information is required for “snooping” breaches
- Most breaches are resolved at the intake stage when the custodian demonstrates it has taken the steps necessary to notify affected parties contain the breach and prevent future breaches


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.

Annual Reports to the Commissioner

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



Annual Statistical Reports to the Commissioner

- Custodians are 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
  - This annual report must also include breaches that do meet the criteria for immediate mandatory reporting to the IPC

Annual Reports to the Commissioner

6.4 (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

Stolen

- Total number of incidents where personal health information was stolen.
- Of the total in this category, the number of incidents where:
  - theft was by an internal party (such as an employee, affiliated health practitioner, or electronic service provider)
  - theft was by a stranger
  - theft was the result of a ransomware attack
  - theft was the result of another type of cyberattack
  - unencrypted portable electronic equipment (such as USB keys or laptops) was stolen
  - paper records were stolen

Lost

- Total number of incidents where personal health information was lost.
- Of the total in this category, the number of incidents where:
  - loss was a result of a ransomware attack
  - loss was the result of another type of cyberattack
  - unencrypted portable electronic equipment (such as USB key or laptop) was lost
  - paper records were lost

Used Without Authority

- Total number of incidents where personal health information was used (e.g. viewed, handled) without authority
- Of the total in this category, the number of incidents where:
  - unauthorized use was through electronic systems
  - unauthorized use was through paper records

Disclosed without Authority

- Total number of incidents where personal health information was disclosed without authority
- Of the total in this category, the number of incidents where:
  - unauthorized disclosure was through misdirected faxes
  - unauthorized disclosure was through misdirected emails

In All Categories

- For each category of breach, the number of incidents where:
  - one individual was affected
  - 2 to 10 individuals were affected
  - 11 to 50 individuals were affected
  - 51 to 100 individuals were affected
  - over 100 individuals were affected

Additional Notes

- Count each breach only once. If one incident includes more than one category, choose the category that it best fits
- Include all thefts, losses, unauthorized uses and disclosures in the year even if they were not required to be reported to the Commissioner at the time they occurred
- Collected through the IPC's Online Statistics Submission website
  - https://statistics.ipc.on.ca/web/site/login

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