Privacy Requirements, Breaches and Reporting

Joshua Shaw, LL.M. J.D.

Health Privacy Policy Analyst
Health Policy Department
Office of the 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

Presentation to the *Association of Ontario Midwives*

October 10, 2018

To whom does *PHIPA* apply?

- Principally, *PHIPA* applies to health information custodians

1. A person or organization described under *PHIPA*
2. who has **custody or control** of personal health information
3. from **performing powers, duties or work** described in *PHIPA* (if any are described)

- Also applies to:

agents of custodians	third parties*
electronic service providers	prescribed entities, persons*
health information network providers	
researchers*	

*who receive personal health information from a custodian

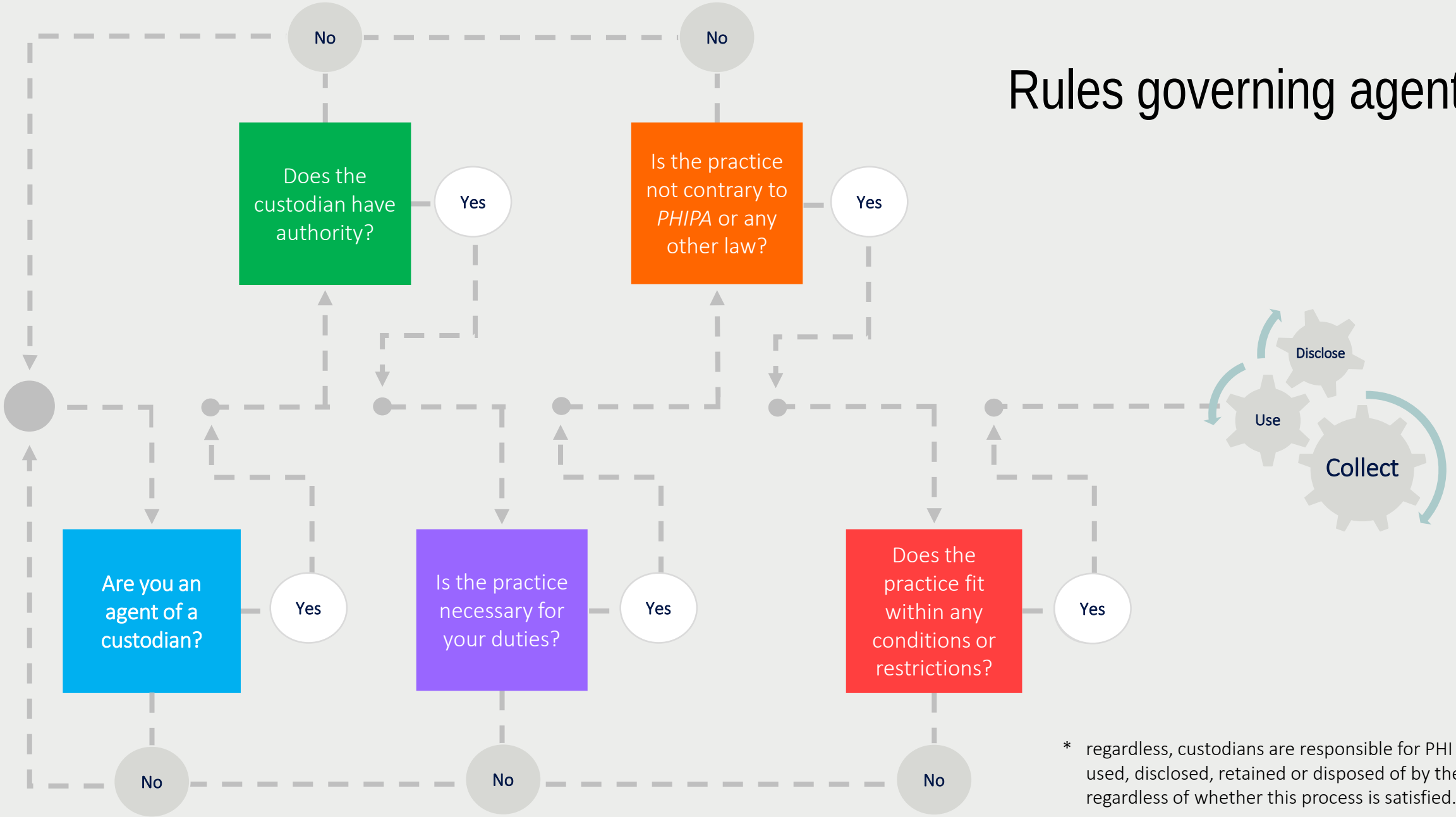
Privacy and security obligations of custodians

Rules for collection, use and disclosure	• **Consent** required for a necessary and lawful collection, use or disclosure, **unless otherwise permitted** or required by *PHIPA*. • Ensure personal health information is **accurate, complete and up-to-date** prior to use • **Minimization** principles put limits on whether personal health information can be collected, used or disclosed: 1. **Cannot** collect, use or disclose personal health information **if other information** will serve that purpose; 2. **Cannot** collect, use or disclose **more than is necessary** for the purpose.

Privacy and security obligations of custodians

Security of PHI	• Take steps to **safeguard personal health information** against:
	  • theft,
	  • loss,
	  • unauthorized collection, use or disclosure, and
	  • unauthorized copying, modification or disposal of records
	• **Notice** to individuals affected by a breach, to regulatory colleges if applicable, and to the IPC
	• Take steps to **ensure agents do not act contrary** to *PHIPA*; responsible for PHI handled by agent

Rules governing agents



* regardless, custodians are responsible for PHI collected, used, disclosed, retained or disposed of by their agents, regardless of whether this process is satisfied.

Consent for collections, uses and disclosures

Express consent

Consent that is clearly and unmistakably given **orally or written**.

Required to:

- Disclose to someone who is not a custodian
- Disclose to another custodian for a purpose other than health care
- Collect, use or disclose for marketing
- Collect, use or disclose for fundraising, if it amounts to more than a name and address

Implied consent

Consent that one concludes has been given based on an **action or inaction.**

Permitted in all other circumstances, where consent is relied upon.

Elements of consent:

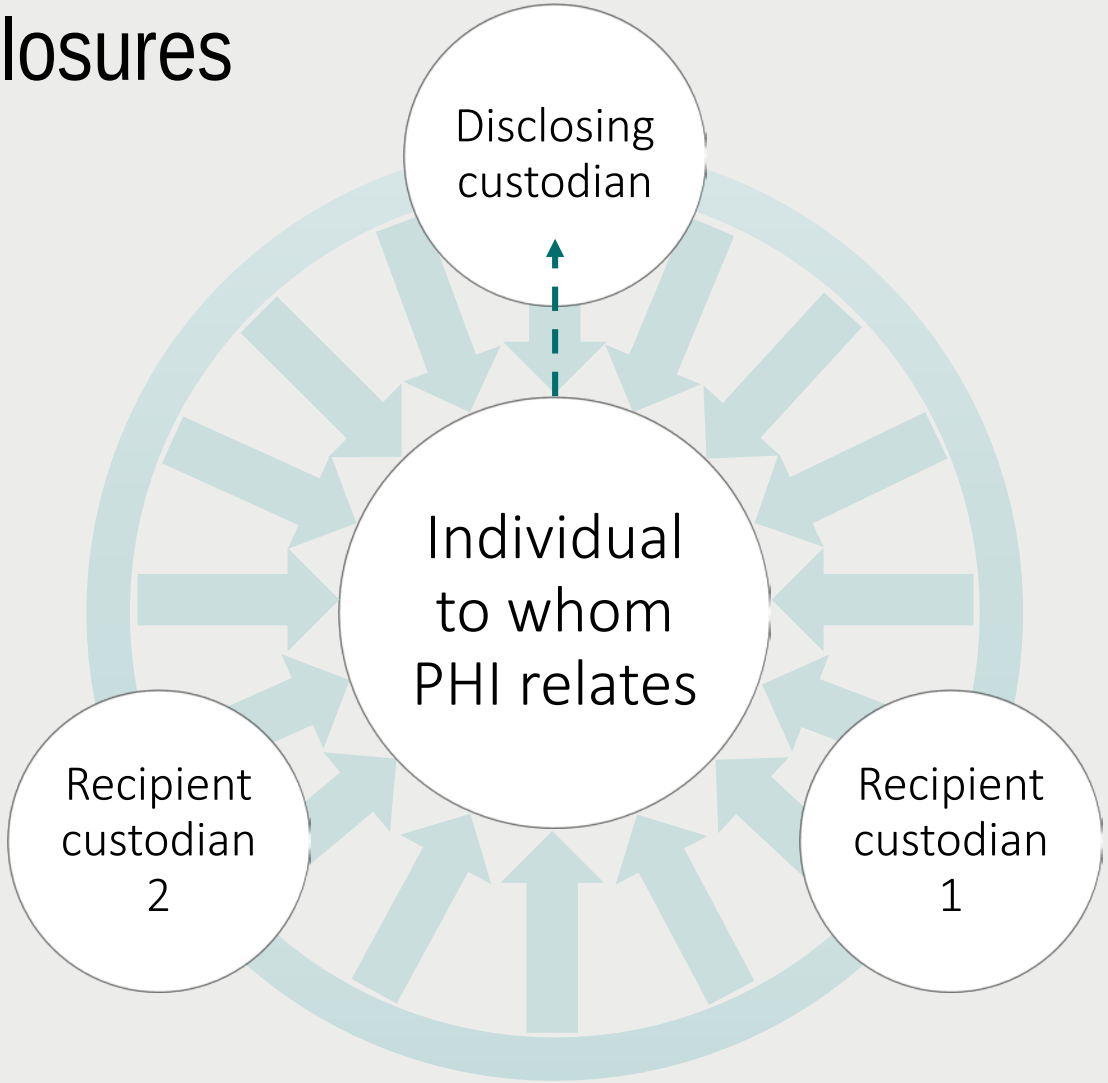
- given by individual or substitute decision maker,
- must be knowledgeable of purpose of the practice, and that they can give or withhold consent
- relate to the information,
- not obtained through deception or coercion

Consent for collections, uses and disclosures

Assumed implied consent

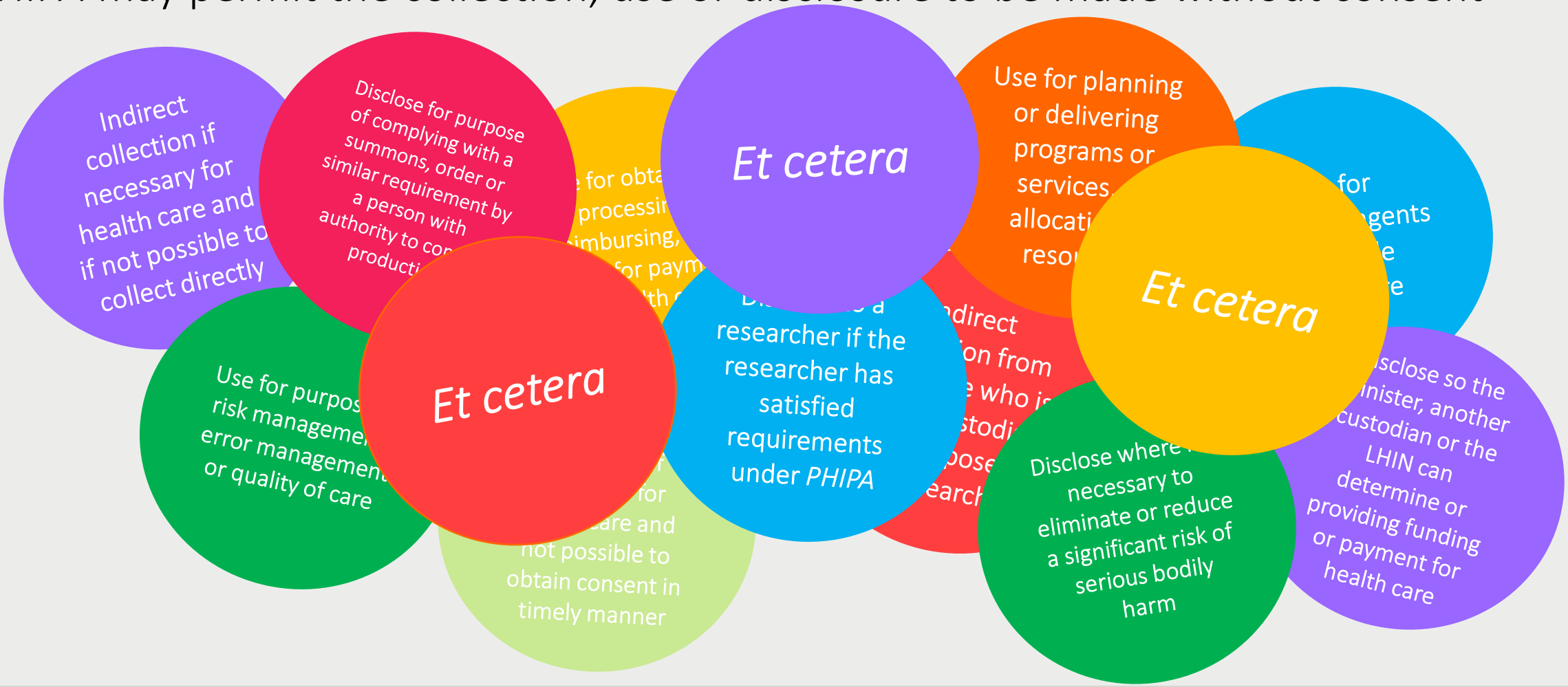
Assume that all elements of consent are fulfilled for collection, use or disclosure

- May only assume if collection, use or disclosure is for **health care**, or assisting in health care.
- Personal health information **received by** certain custodians (and their agents) within the Circle of Care entitled to assume consent.
- Reasonableness of assumption sets **boundaries of the Circle of Care** (e.g., PHIPA Decision 15, Morris (Re), 2015 CanLII 54751 at para. 25.)
- Patient may **withhold or withdraw** consent, putting a stop to assumed implied consent.



Collection, use or disclosure without consent

- *PHIPA* may permit the collection, use or disclosure to be made without consent



Potential cause of privacy breach

Unauthorized access	• When one **views, handles or otherwise deals** with personal health information **without consent** and/or purposes **not permitted** by *PHIPA*
	• To reduce the risk, the custodian should:
	  • explain the purposes for which agents may access and provide **ongoing training**
	  • use confidentiality/ end-user **agreements**, privacy **notices** and privacy **warning flags**
	  • implement access controls (e.g., purpose-driven, data minimization)
	  • log, **monitor** and **audit** access
	• In the event of a breach, **terminate** access privileges immediately and **discipline** appropriately

Potential cause of privacy breach

Shared electronic health records	• Lack of clarity regarding responsibilities in shared electronic health record systems
	  • No custodian has sole custody or control
	• A shared **governance framework**, with **harmonized** privacy policies and procedures:
	  • set out the **roles and responsibilities of each participating** custodian
	  • set out the expectations for **all** custodians and agents accessing system
	  • ensure **all** custodians are operating under common privacy standards
	  • set out how the **rights of individuals** will be exercised

Potential cause of privacy breach

Portability of digitized information	• Portability increases opportunities for breaches, inadvertent or intentional
	• Stop and ask, “Do I really **need** to store personal health information on this device?”
	• Think about the alternatives: Would **de-identified information** serve the purpose? Could the information instead be **accessed remotely** through a **secure connection or virtual private network**?
	• If you need to retain it on a device, protect it by
	  • ensuring it is **encrypted** and protected with strong **passwords**
	  • retaining the least amount of personal health information
	  • developing policies and procedures, train agents and monitor and audit compliance

Potential cause of privacy breach

E-mail communications between custodians	• Communicating **between custodians** via e-mail, similarly, increases opportunity for breaches
	  • IPC expects e-mails to be secured by **use of encryption**.
	  • There may be **exceptional circumstances** where communication of personal health information between custodians through encrypted e-mail may not be practical, such as in an emergency.
	  • Custodians should also look to their **health profession regulatory colleges** for applicable guidelines, standards or regulations on the use of unencrypted e-mail to communicate (e.g., College of Midwives of Ontario has a guideline pertaining to use of electronic communication.)

Potential cause of privacy breach

E-mail communications between custodian and individuals	• Communicating **to patient** via e-mail, may also exacerbate risk to privacy
	  • IPC expects e-mailing to be secured by **use of encryption**, if feasible with the individual to whom the information relates
	  • Where it is not feasible, custodians should consider whether it is **reasonable to communicate** through unencrypted e-mail:
	  • Consider alternative methods
	  • Is this urgent or emergent?
	  • Does the patient expect you to communicate in this way?
	  • How sensitive is the personal health information?
	  • How much personal health information will be, and how frequently will it be communicated?

Potential cause of privacy breach

E-mails generally

Custodians are expected to develop and implement a **written policy and accompanying procedures** for sending and receiving personal health information by e-mail, including reference to

- duties to limit the amount and type of personal health information included in e-mail
- retention and disposal in a secure manner (personal health information should only be stored on e-mail servers and portal devices for as long as it is necessary to serve the intended purpose)
- training and education, privacy breach management system

- **Notify patients about this policy** and **obtain consent prior to communicating** via e-mail if the personal health information will not be encrypted
- Consent may be provided verbally or in writing

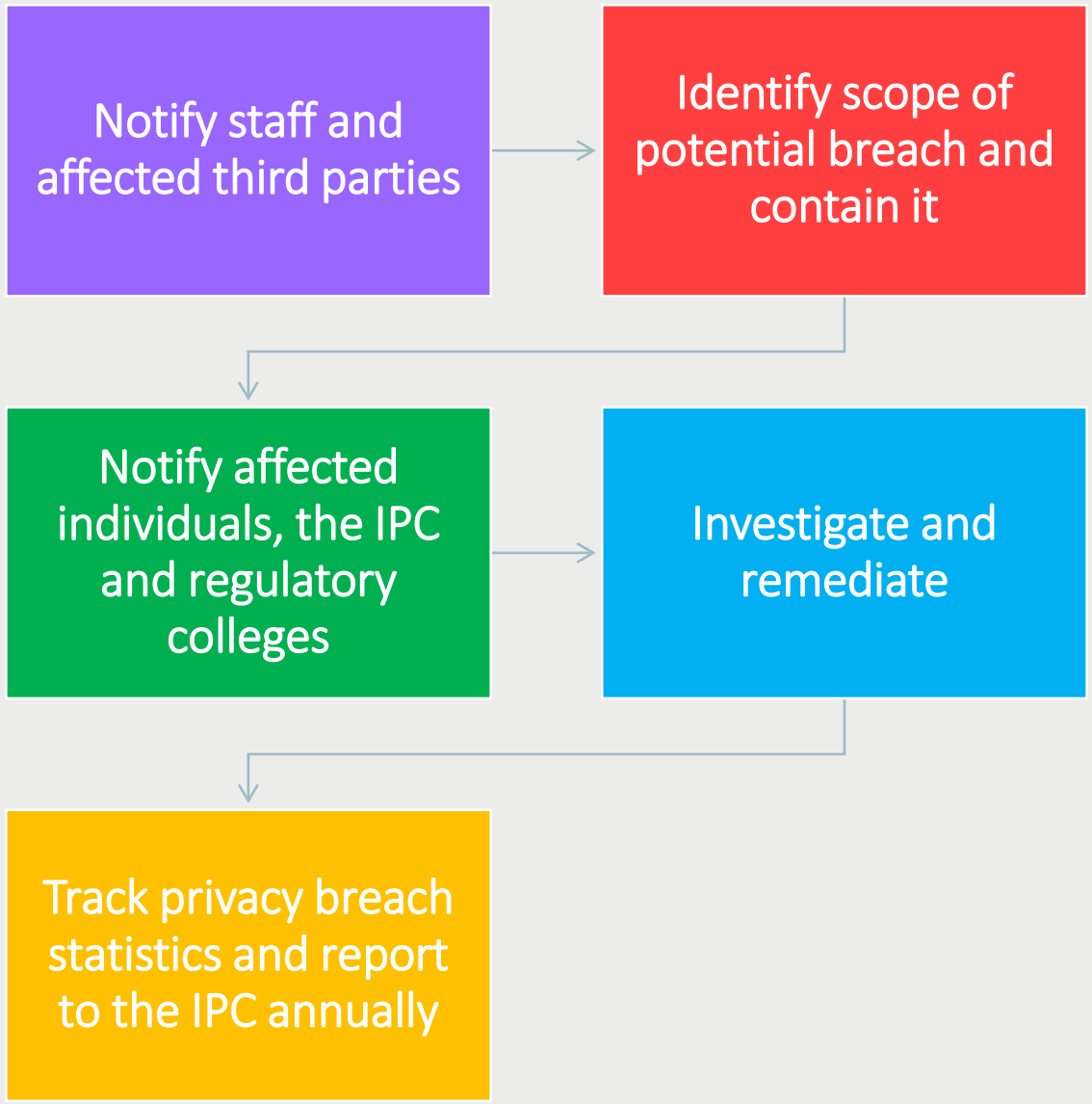
Potential cause of privacy breach

Abandoned health records	• A change in practice can result in abandoned health records • E.g., unexpected death, retirement, relocation, bankruptcy or incapacitation may produce lapses in secure retention or transfer of records • Custodians' security obligations do not end until a legally authorized successor has custody and control of the records – including, duty to securely retain and safeguard records, duty to transfer records, duty to dispose of records, and duty to notify. • Custodians should have a succession plan to prevent abandoned records, which is **routinely updated** and **clearly describes responsibilities** of agents who will give effect to secure transfer to an identified successor

Steps to follow in event of breach

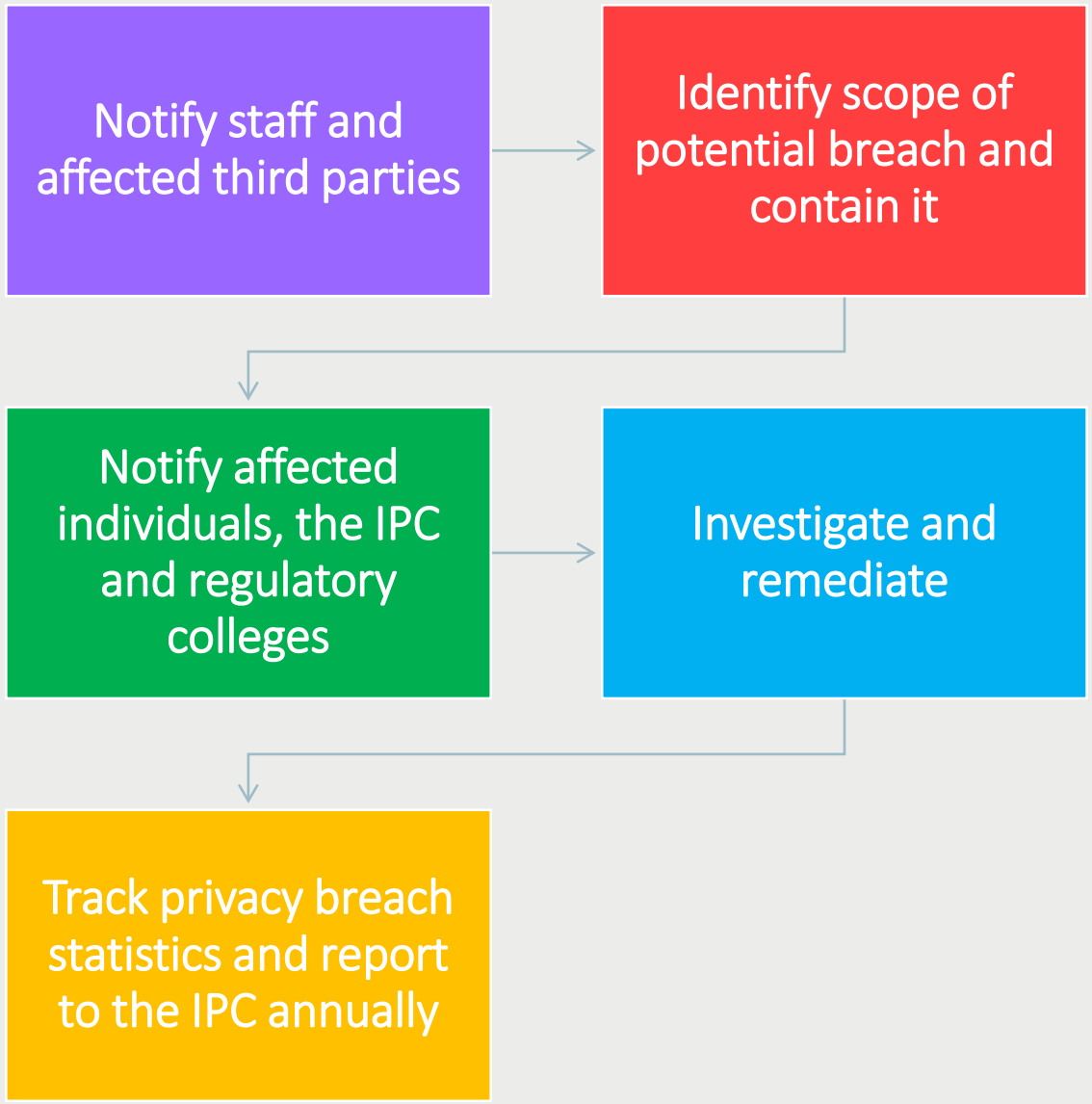
In event of a privacy breach, recommended that custodians have a privacy breach protocol:

- Enables quick, coordinated responses to a breach
- Clarifies roles and responsibilities
- Establishes processes to investigate, contain and remediate a breach
- Prepares the custodian for possible involvement of the IPC in the event of an investigation
- Best situates the custodian, enabling compliance with *PHIPA*



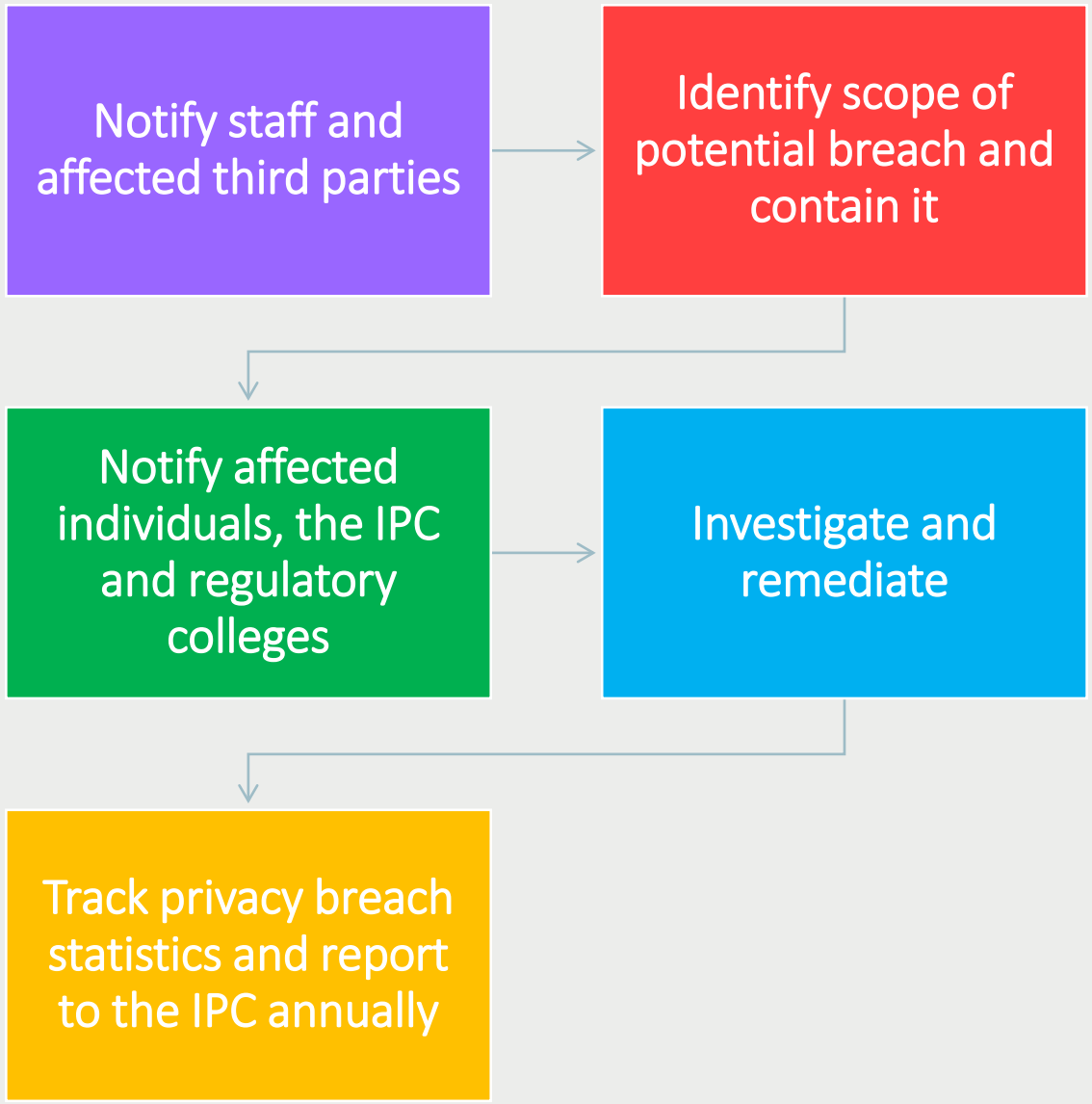
Steps to follow in event of breach

- Notify appropriate staff of breach, including chief privacy officer or other staff member responsible for privacy
- Depending upon nature or seriousness of breach, notify upper management or departments likely to be involved
- In situations with shared electronic systems, notify all affected custodians



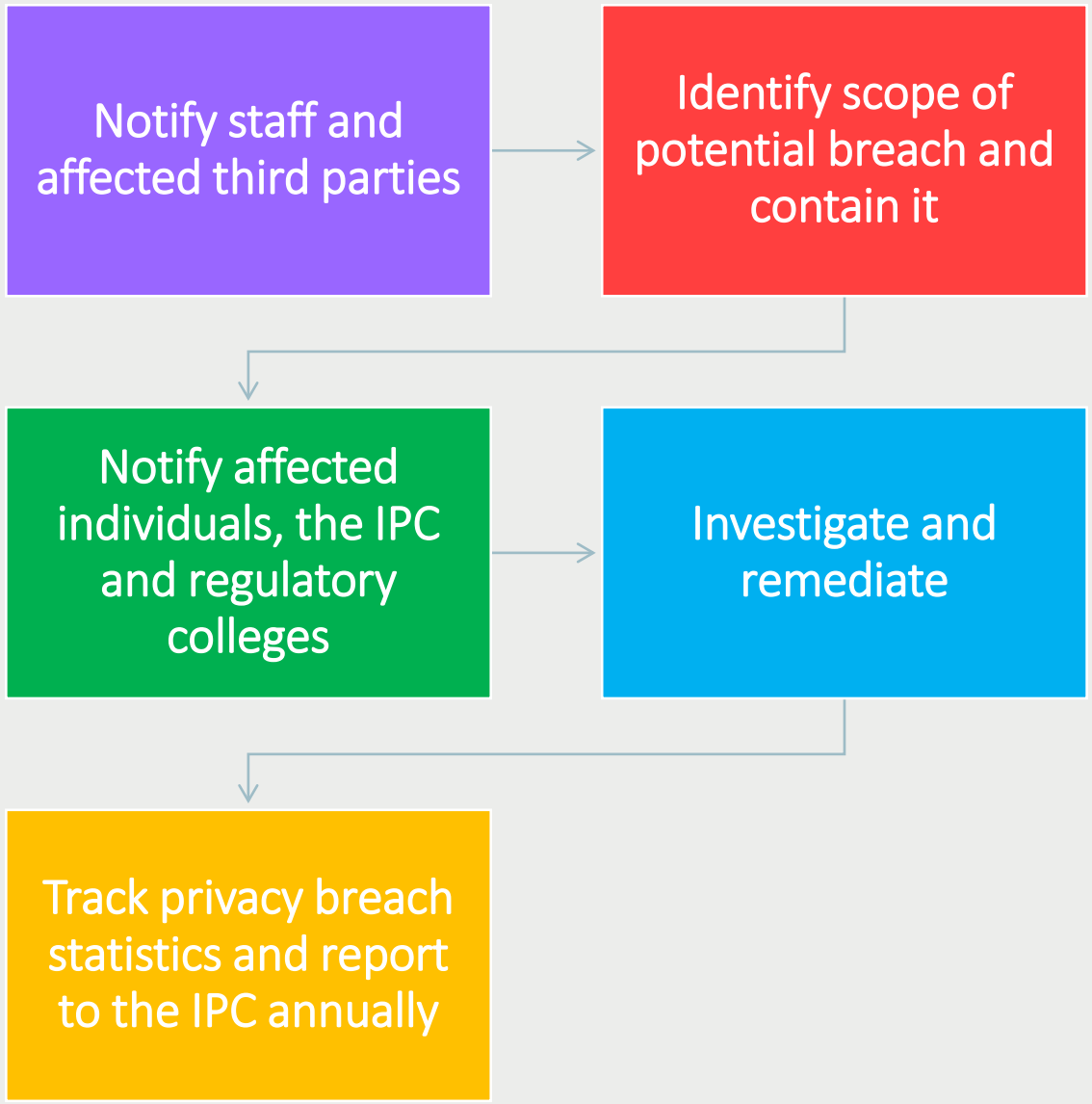
Steps to follow in event of breach

- Identify scope, including:
  - individuals or organizations involved with or responsible for breach
  - nature of PHI
  - quantity of PHI
- Retrieve copies of PHI disclosed
- Ensure no copies were made or retained by anyone not authorized to receive PHI
- Take steps to change passwords, identification numbers or temporarily shutting down system
- Suspend access rights of agents



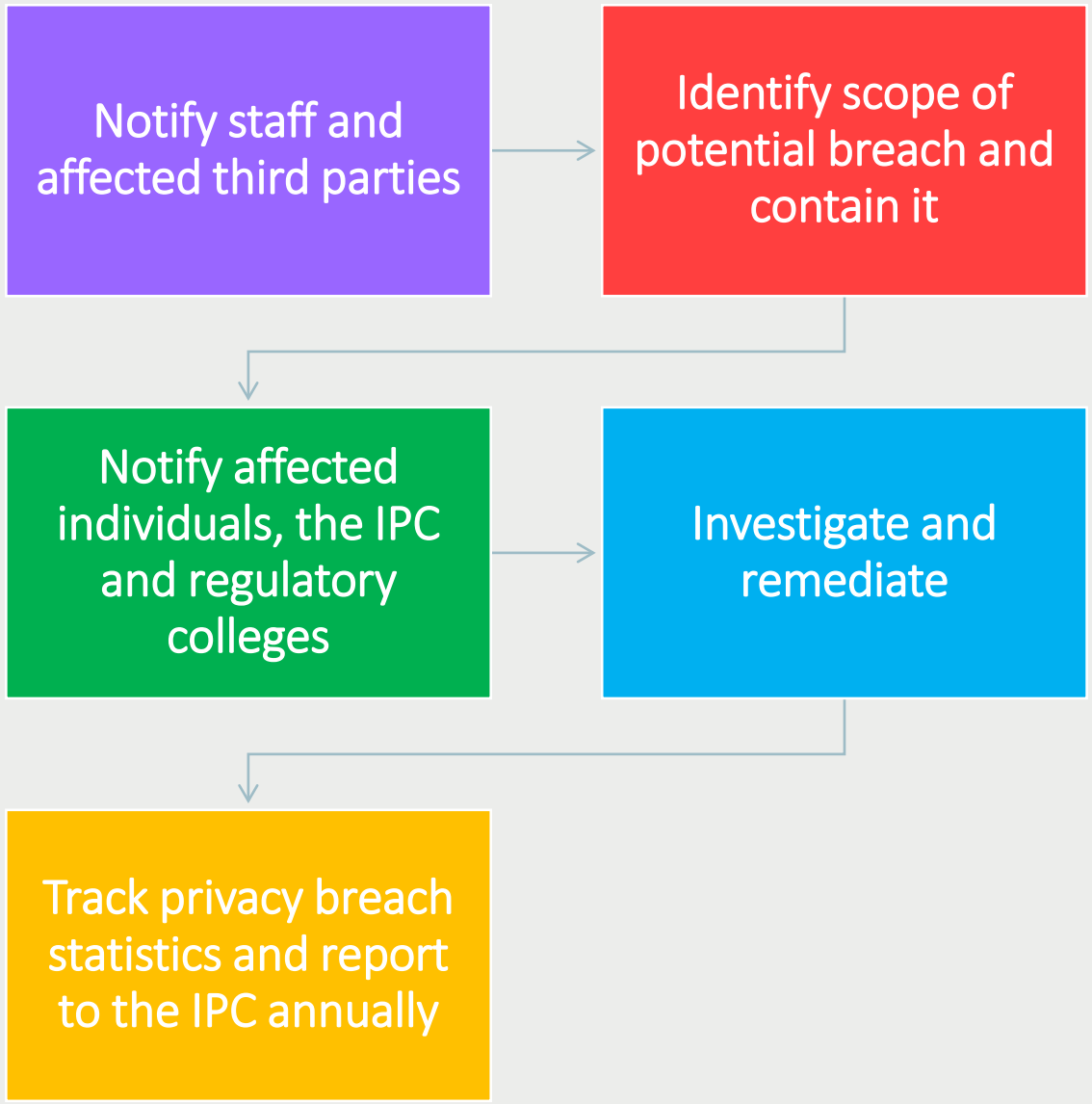
Steps to follow in event of breach

- *PHIPA* requires custodians to notify individuals affected by breach at first reasonable opportunity
- Notice to individuals should provide:
  - Description of nature and scope of breach
  - Description of PHI subject to breach
  - Measures taken to contain breach
  - Name and contact info of person within organization who can address inquiries
- Notice should include statement letting individuals know they can complain to IPC



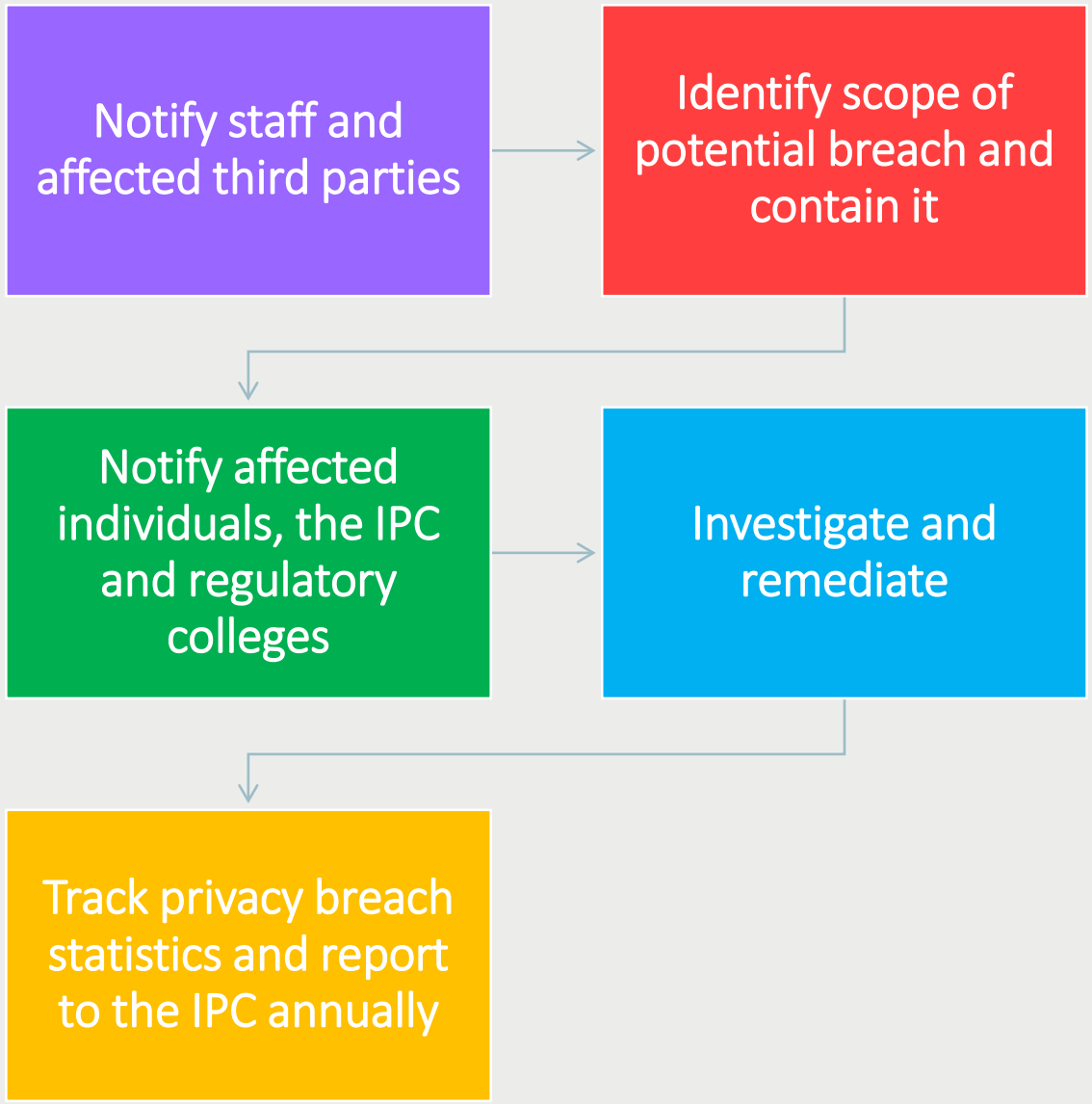
Steps to follow in event of breach

- *PHIPA* now requires custodians to report certain privacy breaches to the IPC. Categories of breaches where reporting is mandatory include:
  - use or disclosure without authority
  - stolen information
  - further use or disclosure without authority after breach
  - pattern of similar breaches
  - disciplinary action against college and non-college members
  - significant breaches
- Also required to report to health profession regulatory colleges



Steps to follow in event of breach

- Conduct an internal investigation to:
  - ensure immediate requirements of containment and notification are met
  - review circumstances of breach
  - review adequacy of existing policies and procedures
- Address breach from systemic basis, including changes to administrative or security controls, and policies or procedures
- Keep log of all privacy breaches
- Consider proactive measures to minimize risk of a privacy breach

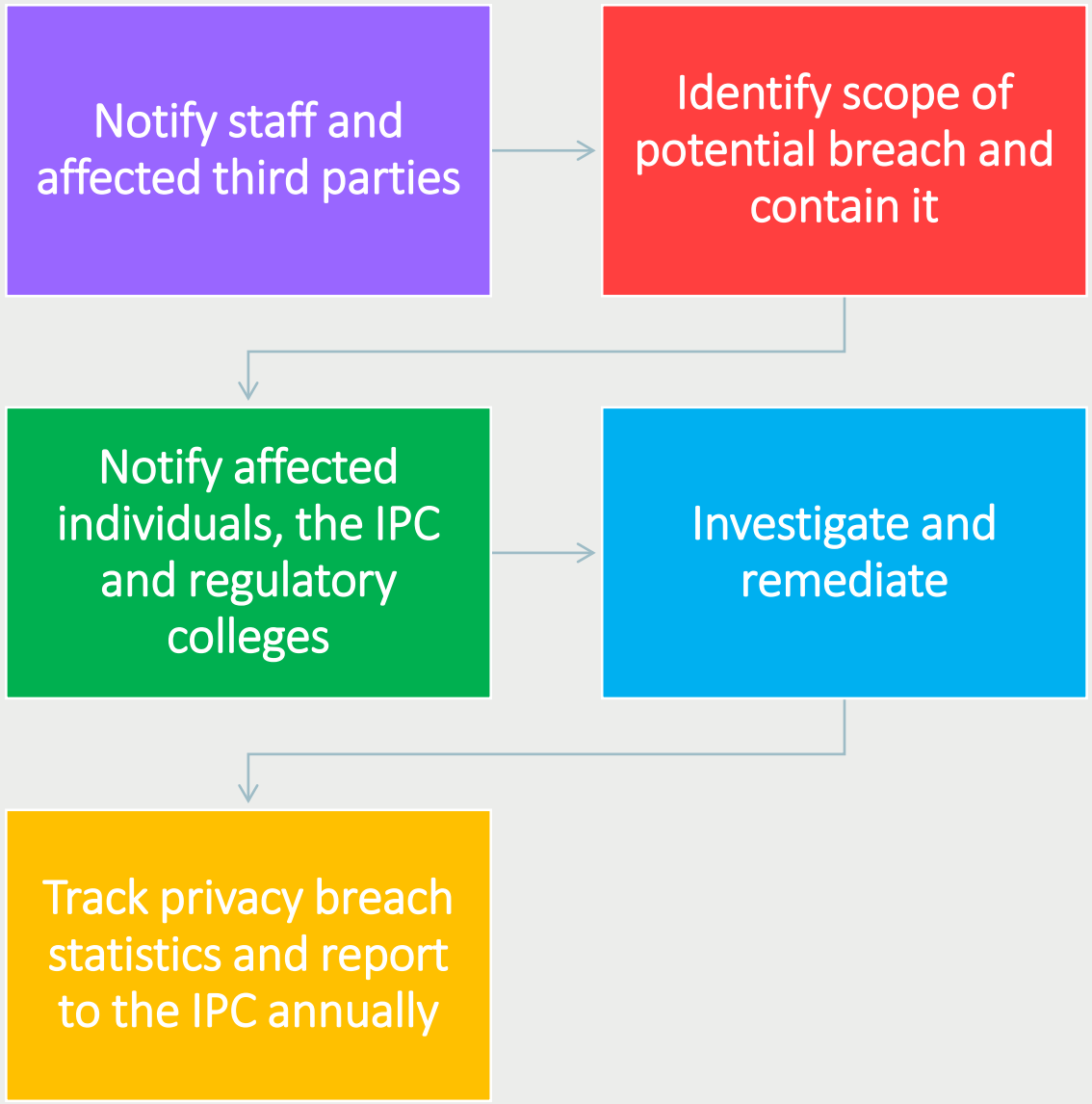


(How to proactively minimize risk of a breach)

- To proactively minimize risk, should:
  - educate staff about privacy rules
  - implement, enforce and routinely update policies and procedures
  - use administrative and technical safeguards to secure PHI
  - ensure no more PHI is collected, used or disclosed
  - ensure that PHI is not collected, used or disclosed if other info will serve purpose
  - conduct privacy impact assessments
  - seek advice from legal counsel, privacy officer internal to organization, or comments from the IPC

Steps to follow in event of breach

- On or before March 1 of each year, starting in 2019, custodians must report statistics about privacy breaches to the IPC, including:
  - PHI stolen
  - PHI lost
  - PHI used without authority
  - PHI disclosed without authority
- The report will be transmitted to the Commissioner by electronic means, through a portal
- Custodians must have started tracking privacy breach statistics as of January 1, 2018



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
josh.shaw@ipc.on.ca

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