BRIGHTSQUID

Mandatory Breach Reporting

Health Information Act – Amendment of regulations

Ingrid Ruys and Rohit Joshi

Agenda

1. A Brief History
2. What Constitutes a Breach?
3. Examples of a Breach
4. HIA Mandatory Breach Reporting Notification – Decision Tree (Flow Chart)
5. HIA – Regulation Amendments for Mandatory Breach Reporting “Assessment” Checklist
6. How to assess the “Risk of Harm”
7. Notices
   a) To the individual
   b) To the Commissioner
   c) To the Minister
8. Offenses and Penalties
9. Seven Steps to Reduce Risk of Breach
10. Brightsquid Help Line & Training Dates

Brief Timeline of Privacy Regulation

2001 – HIA became the law

2011 – **Privacy Impact Assessments required for 8 additional custodians**

Health Information Act (HIA) designated specific healthcare professionals as custodians of health information, increasing the level of privacy required for those professionals.

2013 – **Medicentres breach** (laptop theft with 620,000 patient health files) went unreported for a period of time triggering a legislative change to mandate breach reporting

2014 – **Amendments to the HIA** require reporting for incidents resulting in loss, unauthorized access or disclosure of patient information (known as a '**breach**').

2017 – **Pharmacist sentenced to 3 months house arrest** for improperly access patient information. Pharmacist lost license to practice.

Aug 31, 2018 – **Breach reporting mandatory**

What Constitutes a Breach?

HIA Section 60.1 - identifies two elements of a breach:

1. **Loss of, or unauthorized access** to or disclosure of individually identifying information *and*;

2. **Risk of harm to the individual** who is the subject of the loss, unauthorized access, or disclosure of their information

A **privacy breach** occurs when there is **unauthorized access** to or collection, use, disclosure or disposal of personal information.

Such activity is “unauthorized” if it occurs in contravention of the Freedom of Information and Protection of Privacy Act (FOIP Act), **Health Information Act (HIA)** and Personal Information Protection Act (PIPA).

Examples of a Breach – from an HIA perspective

- **Loss of Patient Information**
  - Misplaced (stolen, lost) laptop or cellphone, misdirected fax or email, patient files lost or destroyed, improper storage, not protected)

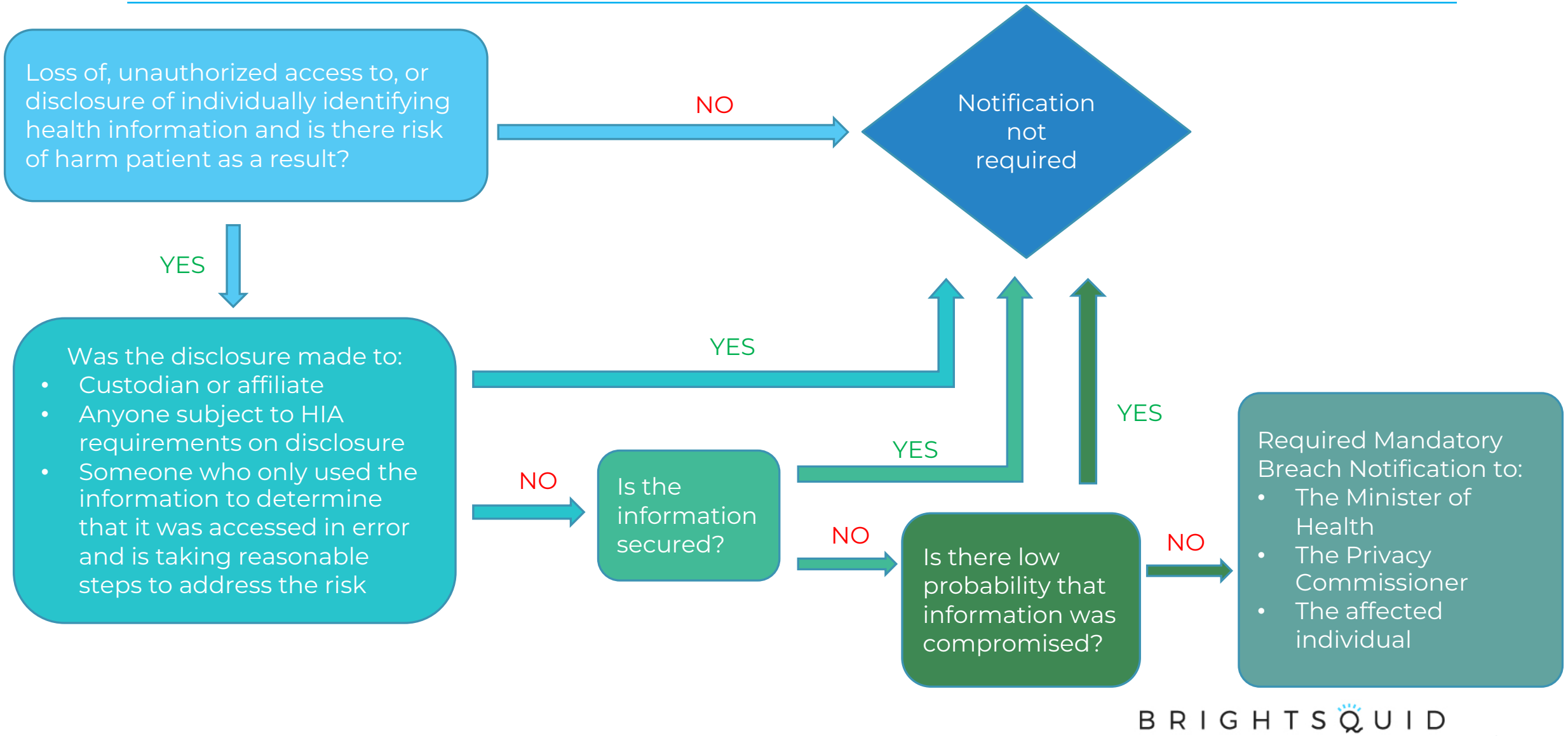
- **Unauthorized Access (Use) of / to Medical Records**
  - Snooping, collecting unnecessary information, inappropriate storage (USB stick, boxes in garage,

- **Disclosure of Patient Information**
  - gossiping, misdirected information, failure to protect

- **Information Technology**
  - No back-up, hacking, cyber-crime, insufficient safe-guards, no agreements in place, non-conformed, mishandling of medical information

BRIGHTSQUID

HIA Mandatory Breach Notification - - Decision Tree



BRIGHTSQUID

HIA Breach – Assessment of Risk of Harm Checklist

Custodian **must** consider the following factors --- ***Reasonable basis to believe*** that:

- ❑information has been or may be accessed by or disclosed to a person;
- ❑that information has been misused or will be misused;
- ❑that information could be used for purpose of identity theft or to commit fraud;
- ❑That the information is the type that could cause embarrassment or physical, mental or financial harm to or financial harm to or damage the reputation of the individual who is the subject of the information;
- ❑Loss of or unauthorized access to or disclosure of information has adversely affected or will adversely affect the provision of a health service to the individual who is subject of the information

HIA Breach – Assessment of Risk of Harm Checklist (cont)

In the case of **Electronic information**, whether the custodian is able to demonstrate that the information was encrypted or otherwise secured in a manner that would:

- ❑ Prevent the information from being accessed by a person who is not authorized to access the info
- ❑ Render the information unintelligible by a person who is not authorized to access the information

In the case of **loss of information** that is subsequently recovered by the custodian, whether the custodian is able to demonstrate that the only person who accessed the information or to whom the information was disclosed

- ❑ Is a custodian or an affiliate
- ❑ Is subject to confidentiality policies and procedures that meet the requirements of s60 of the HIA
- ❑ Accessed the information in a manner that is in accordance with the person's duties as a custodian or affiliate and not for improper purposes, and
- ❑ Did not use or disclose the information except in determining that the information was accessed by or disclosed to the person in error and in taking any steps reasonably necessary to address the unauthorized access or disclosure.

Notice Provisions

If the custodian determines that there is a risk of harm, there is a ***requirement to notify***, as soon as practicable.

Notices must be provided via letter, electronic means, poster in clinic, etc.

1. Notice to the patient(s)
2. Notice to the Privacy Commissioner (OIPC)
3. Notice to the Health Minister

New Offenses & Penalties

Offenses

1. Failure to take reasonable steps to create & maintain administrative, technical and physical safeguards (documented in the Privacy Impact Assessment).

Penalty

1. Fines – Any person found guilty of the above offenses is subject to a fine of up to $50,000
2. Business Impact – Brightsquid's experience with HIPAA legislation in the USA is that the largest impact to the clinic comes from loss of business & reputational damage.

BRIGHTSQUID

Seven Steps to Aid in Reducing Risk of a Breach

1. **Privacy Impact Assessment (PIA) -** will determine what information you have, how you collect use and disclose and provide Policies and Procedures
2. **Risk Mitigation Strategies** – Where are your risks? How can you minimize, reduce or remove risks?
3. **Awareness** – know the current trends (within your Association, medical community) – what are the most common breaches
4. **Training** – keep you and your staff trained and up-to-date on privacy, latest trends and what's new.
5. **IT** – stay up-to-date, ensure strong passwords, security, auditing ability, backup, Agreements
6. **Limit Information –** collect, use and disclose only what is needed, including disposition and storage (ensure proper destruction and storage of medical data / information)
7. **Communications** – ensure secure communications – secure mail, secure fax

Brightsquid is Your Privacy Partner

Complete Compliance Package includes:

- **Complete Privacy Impact Assessment**
  - Includes Policies and Procedures
  - Risk Mitigation and Strategies

- **Training**
  - Calgary – September 28
  - Lethbridge - October 5
  - Red Deer - October 26
  - Edmonton – November 16

- **Privacy Hotline**
- **Breach Reporting Assistance**

AlbertaPIA.ca
privacy@brightsquid.com
800-263-6503 x 301

BRIGHTSQUID