PRACTICE ADVICE

REPORTING PRIVACY BREACHES

EFFECTIVE: JANUARY 2018

REPORTING PRIVACY BREACHES
Samidha Joglekar, Audiology Advisor & Manager of Mentorship
Sarah Chapman-Jay, Practice & Quality Assurance Advisor
Alex Carling, Director of Professional Practice and Quality Assurance

You are required to keep your patients' personal health information (PHI) safe, and confidential. A privacy breach occurs when Ontario's Personal Health Information Protection Act (PHIPA) has been contravened, for example, where personal health information is stolen, lost or if it is used or disclosed without authority.

Health information custodians (HICs) are required to report privacy breaches to the Information and Privacy Commissioner of Ontario (IPC) and certain breaches to the College. Agents must notify the HIC at the first reasonable opportunity if there has been a privacy breach. This article will help you understand your reporting responsibilities.

How do I know if I am a HIC or an agent according to *Personal Health Information and Protection Act* (PHIPA)? Read this…

IPC provides useful resources on how to safeguard PHI, including:

IPC Fact Sheet: Safeguarding Personal Health Information

Insurance companies and the IPC have highlighted cyber security as a concern. If you have electronic records or use cloud storage you are encouraged to consult with information technology experts to ensure secure storage, retention and appropriate destruction of PHI.

WHEN TO NOTIFY THE INFORMATION AND PRIVACY COMMISSIONER (IPC) OF A SECURITY BREACH

To improve the protection and privacy of PHI, the Ontario government has made changes to the *Personal Health Information and Protection Act*. As of October 1st, 2017, HICs and, if appropriate, agents must report breaches to the IPC in seven different categories. 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 or the HIC must make a report.

THE SEVEN TRIGGERS TO NOTIFY THE IPC

1) A person used or disclosed PHI without authority

When the person committing the breach knew, or ought to have known, that their actions were not permitted.

2) PHI was stolen

This could include stolen paper records, or a stolen laptop or other electronic device. You do not need to notify the Commissioner if stolen information was properly de-identified or encrypted.

3) A subsequent breach flows from an initial breach

Following an initial privacy breach, you become aware that the information was or will be further disclosed without authority.

4) Pattern of similar breaches over time

A pattern of similar breaches either at a similar time during the day or by a group of health professionals may reflect a systemic issue that needs to be addressed.

5) Disciplinary action against a College member in connection with a breach

The duty to report to the College also triggers a duty to notify the Commissioner. Where an employee or agent of a HIC is a member of a college you must notify the Commissioner of a privacy breach if:

- You terminate, suspend, or discipline a member as a result of the breach
- The member resigns related to the breach
- You revoke, suspend, or restrict the member's privileges or affiliation as a result of the breach
- The member relinquishes or voluntarily restricts their privileges or affiliation, and this is related to a privacy breach

6) Disciplinary action against a non-college member

Even if your employee is not a College member (e.g., CDA or HIS/HIP), you must still notify the Commissioner in the same circumstances that would have triggered notification to the College.

7) The breach was significant

Use your professional judgement and 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

WHEN TO NOTIFY THE COLLEGE:

You must notify the College as well as the IPC if:

1. An employee is terminated, suspended or subject to disciplinary action as a result of the unauthorized collection, use, disclosure, retention or disposal of personal health information by the employee.

2. An employee resigns and the HIC has reasonable grounds to believe that the resignation is related to an investigation or other action by the custodian with respect to an alleged unauthorized collection, use, disclosure, retention or disposal of personal health information by the employee.

The workplace carries out the initial investigation. The individuals (patients or substitute decision makers) affected by the breach need to be notified by the member or workplace. You need to inform the College and the IPC of the disciplinary action within 30 days. Individuals will be fined $100,000 for a privacy breach. Organizations will be fined $500,000 for a privacy breach.

TAKE HOME MESSAGES:

1. Have a Privacy Breach Plan – The plan should be anticipatory not reactionary. How you handle the breach is more significant to the public than the breach itself.
2. Make sure everyone on your team knows about the plan and their role in the case of a privacy breach.
3. Document the breach

Additional Resources:

Reporting a Privacy Breach to the Commissioner

Preventing and Managing Privacy Breaches

Communicating Personal Health Information by Email

Annual Reporting of Privacy Breach Statistics to the Commissioner

Detecting and Deterring unauthorized access to personal health information

PHIPA Frequently Asked Questions

Quiz Answers:

Scenario 1: 7

Scenario 2: 2, 7

Scenario 3: 1

Scenario 4: 1, 3, 4

Scenario 5: 1, 3, 7

Scenario 6: 5

Scenario 7: 1, 3 ,6, 7

TRY THIS QUIZ!

Which triggers apply to the scenarios below? Remember, more than one trigger can apply. All 7 triggers are covered in the scenarios below.

Scenario 1: An Audiologist accidentally e-mails a patient report to a group e-mail distribution list. The information in the report includes sensitive details about the patient's mental health.

Scenario 2: An SLP's laptop is stolen. The laptop is not encrypted and has patient files that include personal health information such as clients' names, addresses, and details about their health history.

Scenario 3: An SLP working in a hospital accesses an ex-spouse's medical history for no work-related purpose.

Scenario 4: A manager of an SLP department notices that certain patient files are accessed every day around 10:00am. The patients' whose files are being accessed are not receiving SLP services.

Scenario 5: An audiologist accesses a hospital database to find patients with hearing loss and then passes this information to companies that will market services to those patients.

Scenario 6: The manager of the audiology and speech therapy department terminates the audiologist for the PHI breach in scenario 5 and reports this to CASLPO.

Scenario 7: A CDA has an unpleasant encounter with a patient and posts identifying information about the patient on social media. The post is viewed by 52 people. The SLP then suspends the CDA and restricts privileges.