P-29A: Breach Management Protocol

A privacy breach occurs when there is unauthorized access to, or collection, use, disclosure or disposal of Personal Health Information whether done deliberately or inadvertently. Such activity is unauthorized if it occurs in contravention of the Ontario PHIPA (PHIPA) or BORN policies and procedures

Examples of privacy breaches include instances where Personal Health Information is lost, stolen, or mistakenly provided to the wrong person, such as when a computer is stolen.

Responding to a Privacy Breach

- It is important for all BORN staff to respond immediately when faced with a breach or a potential breach.
- The following steps should be carried out simultaneously or in quick succession:

1. Contain the Breach to the extent possible

As an Agent who discovers a potential breach you should act quickly to limit the breach.

- You must ensure that no further breaches can occur through the same means (e.g., change passwords, identification numbers, and or temporarily shut down a system)
- You must determine what (if any) Personal Health Information has been stolen, lost or accessed, used, disclosed, copied, modified or disposed of in an unauthorized manner
- You must securely retrieve or destroy as much as possible of the breached information. In other words, if the information can be retrieved in a secure fashion, do so, otherwise confirm that as much of the information as is possible has been destroyed, and you have written confirmation of that action including date, time and method of secure disposal
- You must ensure that no copies of the Personal Health Information have been made or retained by the individual who was not authorized to retrieve or receive the information
- You must determine whether the breach or potential breach would allow unauthorized access to any other data (e.g. passwords being disclosed that could provide access to systems or databases) and take whatever steps are necessary and appropriate to shut down that access (e.g. disable the password)

2. Get Help to Evaluate the Situation

As an Agent who discovers a potential breach you are required to support the evaluation of the situation.

- You must notify the Privacy Officer at the first reasonable opportunity

- You must complete and Breach Reporting Form which includes the following:
    - Name and position of the individual who discovered the breach
    - Date and time of discovery
    - Estimated time and date the breach occurred
    - Type of breach (loss, theft, inadvertent disclosure)
    - Cause of breach, if known
    - Description of information involved in the breach
    - Actions taken by Agent reporting the breach to contain the breach
    - Any other individuals or organizations involved in the breach (or its notification) and contact information for relevant individuals
- The Breach Reporting Form should be completed and forwarded to the Privacy Officer as soon as reasonably possible.
- The Privacy Officer will work with you and other appropriate BORN staff or external resources to determine the extent of the breach:
    - What data elements have been breached?
    - Is there a risk of further exposure of the information?
    - Is the information encrypted or otherwise non-accessible?
    - How many individuals are affected by the breach?
    - Who are the individuals affected by the breach?
    - What is the cause of the breach?
    - What organizations are involved in the breach?
- The Privacy Officer, together with you and other appropriate BORN staff or external resources must determine harm that may result from the breach, including:
    - Security risk
    - Identity theft or fraud
    - Hurt, humiliation, damage to individual's reputation
    - Risk to public health

3. Consider Notification

The Privacy Officer will consider broader notification of the breach.

- The Privacy Officer must consider the advisability of notifying other organizations such as:
    - Information and Privacy Commissioner of Ontario
    - Police
- Whenever personal health information is or is believed to be stolen, lost or accessed by unauthorized persons and whenever required pursuant to the agreement with the health information custodian or organization, the Privacy Officer must send written notification to the heath information custodians or organization who provided the information at the first reasonable opportunity in order that they may notify individuals whose privacy was breached.

4. Prevent further breaches

The Privacy Officer is responsible for preventing further breaches.

- The Privacy Officer must review existing policy for necessary changes to BORN policies and procedures to avoid any further breaches
- The Privacy Officer must undertake any required educational campaign within BORN (and associated organizations as necessary) to educate employees on how to avoid further breaches
- The Privacy Officer must review BORN Breach Management Protocol for potential improvements
- The Privacy Officer must take appropriate action regarding the individual responsible for the breach