Privacy Breach Reporting Guidelines

What is a privacy breach?

Privacy breach is not defined by the *FOIPP Act* or *HIA*. Generally, it means any unauthorized collection, use, or disclosure of PHI or PI. If PHI/PI is stolen, lost, or disposed of (except as permitted by the *FOIPP Act* or *HIA*), or is disclosed to, or accessed by, an unauthorized person, notification is usually required.

Acronym Alert:

AI – Affected Individual(s)

HIA – Health Information Act

FOIPP Act – Freedom of Information and Protection of Privacy Act

PHI – personal health information

PI – personal information

Who to notify and when?

The *HIA* has mandatory reporting for breaches while the *FOIPP Act* does not. We encourage Public Bodies to voluntarily report breaches for transparency.

In the event of a privacy breach, custodians under the *HIA* are required to notify the individual to whom the PHI relates, and the Commissioner, at the first reasonable opportunity, unless the custodian reasonably believes that the privacy breach will not have an adverse impact on the individual's:

- o the provision of health care
- o other benefits
- o mental well-being
- o physical well-being
- o economic well being
- o social well-being

Notifications to the AIs and the Commissioner must be in writing. Notification to the AI should contain information on when the breach occurred and the circumstances, with notice that the AI can contact the Commissioner's office to request a review of the breach. For notification to the Commissioner, we provide a form on our website (www.oipc.pe.ca). When completed, this form should provide the necessary background information of the privacy breach. Breach notification is not a Breach Investigation Report.

While breach reporting under the *FOIPP Act* is voluntary, the process for reporting to the Commissioner is the same as *HIA.*

What are the steps of Breach Investigation and Reporting?

The Commissioner will review the custodian's response to the privacy breach. Although responses to privacy breaches may vary, depending upon the unique circumstances of each breach, there are four actions which the Commissioner expects a custodian to take, as follows:

1. Breach Notification
2. Breach Containment
3. Breach Investigation
4. Remediation

After these steps are taken, the Custodian must prepare a written Breach Investigation Report and submit it to the Commissioner, outlining all the steps taken, the investigation findings, and remediation taken or planned.

Breach Notification

When a breach is discovered, the custodian must notify the Commissioner and the AI as soon as reasonably possible. Part of the timely response includes the statutory obligation to notify the individual(s) affected by the privacy breach in writing. It is also advisable to provide an explanation of the circumstances of the breach to the individual, if possible. The Commissioner will ask that the custodian confirm that the affected individual was notified, and for a copy of the notification.

Notification to the Commissioner of the breach is to be made in writing as well. If helpful, we have a Report a Privacy Breach form for each of the *HIA* and the *FOIPP Act* on our website (www.oipc.pe.ca).

Breach Containment

Containment of the breach involves ensuring, if possible, that the PHI/PI at issue is not subject to further unauthorized collection, use, or disclosure. This requires quick action, and a prompt investigation by the custodian. If the PHI/PI was inadvertently sent to the wrong individual, for example, the custodian should retrieve the PHI/PI and inquire about whether copies or other disclosures have been made.

Breach Investigation

The custodian should conduct an internal investigation, to determine precisely how the breach occurred. This is essential for remediation. The custodian is expected to determine the root cause of the breach, such as whether the breach was an oversight, a technical error, or a result of a lack of sensitivity to PHI/PI protection. The Custodian is expected to compile this information into a Breach Investigation Report.

The Commissioner requires a copy of this investigation report to be submitted to the Office of the Information and Privacy Commissioner. There is no standard format for this investigation report, however, it must be in writing and must contain information on the root cause of the breach, the containment of the breach, notification to AI, as well as any and all remediation taken or planned.

Remediation

Remediation is an important step in the breach management process. This may involve staff education, or implementing a more privacy-sensitive office process. There may be a technical solution. Involving staff in the remediation process may better identify gaps in privacy protection and result in finding the best solutions. Even with reasonable safeguards, a custodian may still experience a privacy breach. A privacy breach may reveal gaps that should be addressed. The Commissioner will require the custodian's findings under this step, and may make recommendations for remediation, suggesting safeguards which could be put in place to prevent such a breach, and the resulting impacts, from occurring in future.