Privacy Breach Reporting

Guidelines

PEI Office of the Information and Privacy Commissioner

What is a privacy breach?

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

Acronym Alert:

HIA – *Health Information Act*
PHI – personal health information

When is breach notification required?

In the event of a privacy breach, custodians 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 provision of health care
- other benefits
- mental well-being
- physical well-being
- economic well being
- social well-being

of the individual to whom the PHI relates.

Notification to the Commissioner must be in writing. Although the contents of the notification are not prescribed by the *HIA*, the Office of the Information and Privacy Commissioner provides a form on our website (www.oipc.pe.ca) to submit to the Commissioner. When completed, this form should provide the necessary background information of the privacy breach.

What additional information will the Commissioner require?

The Commissioner will conduct a review of the custodian's breach management procedure, as it relates 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:

Breach Notification
If a breach is discovered, the custodian is expected to respond to the breach as soon as reasonably possible. Part of the timely response includes the statutory obligation to notify the individual(s) affected by the privacy breach. 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 will ask for the content of the notification.

Breach Containment
Containment of the breach involves ensuring, if possible, that the PHI 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 was inadvertently sent to the wrong individual, for example, the custodian should retrieve the PHI 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 protection.

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.