Privacy Breach Procedure Template

Guidance: The information provided below relates to privacy breaches under PIPEDA. Be aware that some provinces with "substantially similar" legislation have notification requirements. You must be aware of the specific provincial requirements where you do business.

A privacy breach occurs when there is an unauthorized access to, or collection, use or disclosure of personal information (PI) that contravenes privacy legislation. Typically breaches occur because PI is lost, stolen, disclosed in error or as a consequence of an operational breakdown.

Procedure to Follow for Privacy Breaches:

- Notify your Compliance Officer and most senior person immediately.
- Gather information about the incident:
    - Date of occurrence
    - Date discovered
    - How discovered
    - Location of the incident
    - Cause of the incident
    - Any other information you can quickly assemble
- **Contain the breach immediately** – don't let any more information escape.
    - Stop the unauthorized practice
    - Recover the records
    - Shut down the system that was breached
    - Revoke or change computer access codes or
    - Correct weaknesses in physical or electronic security.
- **Assess the breach**.
- **Notify the police if the breach appears to involve theft or other criminal activity**. Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause or allow you to take appropriate corrective action."
- **If customer information was involved, notify the MGA and Insurers involved and work with them to determine who needs to be apprised** of the incident internally and externally. Seek instructions on how the insurer would like to proceed. The insurer should determine whether affected individuals should be notified, how they will be notified and by whom. The Privacy Commissioner states "Typically, the organization that has a direct relationship with the customer, client or employee should notify the affected individuals, including when the breach occurs at a third party service provider that has been contracted to maintain or process the personal information." The decision as to whether to notify the affected individuals may have to be delayed in order for a full risk assessment to be conducted.
- Evaluate the risks associated with the breach. Find out:
    a. What PI was involved
    b. How sensitive the information is. Generally, the more sensitive the information, the higher risk of harm. Consider these high risk forms of PI:
        - Health information
        - Government-issued ID such as SINs, driver's license and health care numbers

    - Bank account and credit card numbers
    - If a combination of PI was involved, as this is typically more sensitive. The combination of certain types of sensitive PI along with name, address and DOB suggest a higher risk.
  c. How this PI can be used. Can it be used for fraud or other harmful purposes (i.e. identity theft, financial loss, loss of business or employment opportunities, humiliation, damage to reputation or relationships)?
  d. Is there a reasonable risk of identity theft or fraud (usually because of the type of information lost, such as an individual's name and address together with government-issued identification numbers or date of birth)?
  e. Is there a risk of physical harm (if the loss puts an individual at risk of physical harm, stalking or harassment)?
  f. Is there a risk of humiliation or damage to the individual's reputation (e.g., does the PI include mental health, medical or disciplinary records)?
  g. Whether the PI was adequately encrypted, made anonymous or otherwise not easily accessible.
  h. What is the ability of the individual to avoid or mitigate possible harm?
  i. The cause of the breach.
  j. The extent of the breach – how many individuals have been affected?
  k. Who are they?
  l. What harm can result to your practice? (Loss of trust, assets, financial exposure, legal proceedings).
- Do a thorough post mortem in order to prevent future breaches. What steps are needed to correct the problem? Is this a one-off issue or is it systemic?

If employee information was involved, there will likely be no need to notify the insurers, but follow the same steps as above with appropriate consideration given to the special sensitivities around employee and PI.