

Reporting a Suspected Privacy Breach

Steps for reporting a suspected breach:

If you suspect a potential privacy breach has occurred, please take the following steps in accordance with the *Access to Information and Protection of Privacy Act*:

- 1) Take steps to **CONTAIN** the suspected breach.

What is containment?

Containment consists of steps that an employee can take to reduce or stop the suspected breach from occurring. Examples of containments actions are:

- Immediately recovering the information and have recipient confirm – in writing – that no copies of the information were made, the information was not and will not be communicated, and all copies have been securely destroyed;
- Shutting down the system that was breached;
- Revoking or changing computer access code; or
- Contacting your Designated Privacy Officer.

- 2) **NOTIFY** your Designated Privacy Officer or the ATIPP Office.
- 3) **COMPLETE** the required Privacy Breach Reporting Form for Employees and submit it to your Designated Privacy Officer.

Do not take any additional steps outside of your immediate containment actions until you receive specific written direction from your Designated Privacy Officer or the ATIPP Office.

Do not discuss the suspected breach and do not panic.



What happens next?

ASSESSMENT: Your Designated Privacy Officer will work with you to confirm whether a breach has occurred. You may be provided with additional containment measures and asked to provide additional information to assist with the determination of facts.

If your Designated Privacy Officer confirms a breach has occurred, it will trigger an **INVESTIGATION**.

Investigations are part of the ATIPP Act Protocol and are used to inform better privacy practices to reduce or prevent future breaches.

NOTICE TO AFFECTED PARTIES: If your Designated Privacy Officer determines a breach occurred, affected parties along with the ATIPP Office, Senior Management and other individuals as required (ICT, RCMP, etc.) may be notified according to the scope of the breach and determination of harm.

CONTAINMENT & MITIGATION: Depending on the scope of the breach, containment measures may be broad. You may receive additional requests from your Designated Privacy Officer through the process.

Once the investigation is complete, your Designated Privacy Officer may provide additional mitigation recommendations and a time frame for implementation.

The ATIPP Office provides advice and guidance to public bodies and Designated Privacy Officers.

At any point in the process, you may contact the office for assistance with the breach process, assessments, investigations, notifications and reporting.

For assistance, please contact the ATIPP Office.