SAMPLE
Breach Protocol

Disclaimer to Custodians: This is a sample only.
It may not be suitable for your circumstances and should not be relied on as legal advice.

What is the purpose of the protocol?

This protocol is designed to assist _____ *(name of Custodian)* employees by defining the process to manage breaches. This protocol will provide guidance on:

- timelines when managing breaches;
- determining risk of harm; and
- notification, including who, when and how notification should occur.

What is a breach? (*Health Information Privacy and Management Act* (*HIPMA*) Part 3 Divisions 1, 3, 4)

A breach occurs if there is a theft or loss of information or unauthorized disclosure of, or access to, personal health information (PHI) contrary to *HIPMA*.

Breaches include, but are not limited to:

- misdirected faxes, emails or mail;
- looking up information of neighbours, friends, family, staff and other individual without a job related purpose;
- theft, loss or disappearance of electronic or paper based records;
- inappropriate destruction of PHI information;
- being overheard discussing PHI of a client in a public setting with someone who does not need to know; and
- sharing a story with identifying client information on social media without consent.

STEP 1: Contain the Breach

Recommended Timeline: Immediately

Immediately stop the unauthorized practice, recover the records and/or shut down or correct weaknesses in physical security.

If uncertain whether a breach has occurred, contact the _____ *(position/title of the individual responsible for responding to breaches)*.

STEP 2: Notify the _____ *(position/title of the individual responsible for responding to breaches)*

Recommended Timeline: Same day the breach is discovered.

- All breaches, real or suspected must be reported immediately to the _____ *(position/title of the individual responsible for responding to breaches)*.

- The _____ *(position/title of the individual responsible for responding to breaches)* will begin completing the Breach Reporting Form.
- The _____ *(position/title of the individual responsible for responding to breaches)* will determine who will be the lead in conducting the investigation and completing the Breach Reporting Form.

STEP 3: Determine the risk of harm to affected individuals

Recommended timeline: Within five working days after breach was discovered

- The _____ *(position/title of the individual responsible for responding to breaches)* or delegate completes section 2 of the Breach Reporting Form.
- Refer to the Breach Reporting Form, question 2.3 to assist in determining the sensitivity of the information and the risk of harm.

STEP 4: Notification

Recommended timeline: Within 2–3 weeks after breach was discovered

- The _____ *(position/title of the individual responsible for responding to breaches)* will determine whether notification is required or appropriate. Use the parameters outlined in question 2.4 of the Breach Reporting Form when making this determination.

Determining likelihood of significant harm.

- If there is a likelihood of significant harm, affected individuals MUST be notified as soon as reasonably possible. (*Health Information Privacy and Management Act* ss.30(1))
- In addition, Yukon's Information and Privacy Commissioner must be notified and within a reasonable timeframe, receive a written report that:
  - ➞ assesses the risk of harm to individuals;
  - ➞ estimated number of individuals affected;
  - ➞ measures taken to reduce risk of harm to individuals; and

  (Health Information Privacy and Management Act para. 30(2)(b)) and s. 31).

Determining there is not a likelihood of significant harm.

- If it is determined that there is not a likelihood of significant harm, _____ *(Name of Custodian)* is not obliged to notify affected individuals or the Yukon's Information and Privacy Commissioner. However, best practice is to develop a mitigation strategy to prevent similar future breaches.