SAMPLE
Breach Reporting Form

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.

1. Containment of breach

Name of Custodian: _____ Reported by: _____

Date breach occurred: _____ (YYYY-MM-DD) Date breach was discovered: _____ (YYYY-MM-DD)

1.1 Has there been a breach involving "personal health information"?

A breach occurs if there is a theft or loss of information or unauthorized disclosure of, or access to, PHI contrary to *HIPMA*. Some examples of situations where a breach occurred are:

- misdirected faxes, emails or mail
- looking up information of neighbours, friends, family, staff and other individuals without a job related purpose
- theft, loss or disappearance of electronic or paper based records

Answer:

If you determined a breach has occurred, list the types of information involved. (Refer to Appendix A)

_____

_____

_____

_____

1.2 List the immediate containment actions

Some 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 the _____ *(position/title of the individual responsible for responding to breaches)*.

Answer:

_____

_____

_____

_____

2. Risk of harm

2.1 What is the cause and extent of the breach?

Include the following when answering:

- What is the cause of the breach?
- Is there a risk of ongoing or further exposure of the information?
- Was the information lost or stolen?
- Is the information encrypted?
- Is there a suspicion of malicious intent behind the breach?
- How much information (# of documents or amount of data) was involved in the breach?

Answer:

2.2 How many individuals are affected?

Consider the following when responding:

- Very few (less than 10)
- Identified and limited group (>10 and <50)
- Large number of individuals affected (>50)
- Numbers are not known

Answer:

2.3 What is the sensitivity of the information and what type(s) of harm could occur?

PART 1 — Determine the Sensitivity of the Information

Types of **highly sensitive** information: SIN, date-of-birth, driver's license number, credit card numbers, signatures, medical information (psychiatric or addition counselling notes, for example), employee information (poor performance or termination information, for example). This is not an exhaustive list.

Types of **low or moderately sensitive** information: names, phone numbers, email addresses, and bank accounts. This is not an exhaustive list.

PART 2 — Determine Harm

Harm to the individual:

- **Risk of identity theft**: Most likely when the breach includes loss of SIN, credit card number, driver's licence number, debit card information, a combination of name, date-of-birth and address, etc.
- **Risk of physical harm**: When the information places the individual at risk of physical harm from stalking or harassment.
- **Risk of hurt, humiliation, and damage to reputation**: Often associated with the loss of information such as mental health records, medical records, criminal history or disciplinary records.
- **Loss of business or employment opportunities**: Where the breach could affect the business reputation of an individual.

Harm to the organization:

- **Risk to organization**: Where the organization is concerned that the breach will undermine trust of citizens, loss of assets, financial exposure or contractual and/or legal obligations.

Answer:

2.4 What is the likelihood that significant harm could result?

Consider **all** of the following:

- The length of time between the breach and its discovery;
- The likelihood that there has been any disclosure, unauthorized use or copying of the information;
- The information available regarding the individual's circumstances;
- The likelihood that the information could be used for identity theft or identity fraud;
- The number of other individuals whose information is or may be similarly affected;
- The relationship between the affected individuals and any individuals who has accessed the information. (This is a factor in a small jurisdiction such as the Yukon.); and
- The immediate containment measures taken.

Answer:

3. Notification

3.1 Will affected individuals be notified? If not, why not?

Note: If there is a risk of significant harm you must notify the affected individuals, while at the same time give the Office of the Information and Privacy Commissioner a copy of the notice.

When notifying affected individuals, your notice must include:

- A description of the circumstances of the breach and the information involved;
- Indicate when the breach occurred;
- Describe the measures, if any, that has been taken to reduce the risk of harm to the individual as a result of the breach; and
- Identify who can be contacted within your organisation with questions.
- Notify individuals of their right to complain to the Office of the Information and Privacy Commissioner.

Answer:

4. Prevention

4.1 Describe the physical security safeguards in place.

Describe only those safeguards which relate to the breach. For example: locked cabinets, securely stored laptops, key card access to the building, etc.

Answer:

4.2 Describe the technical security safeguards in place.

Describe only those safeguards which relate to the breach. For example: document encryption, user access profiles assigned and removed on a need-to-know basis, etc.

Answer:

4.3 Describe the administrative security safeguards in place.

Describe only those safeguards which relate to the breach. For example: what security policies will be used to ensure the personal information is protected; what training or procedures are in place so users are aware of access rules.

Answer:

4.4 What internal improvements to processes, systems, policies, and any other actions to mitigate recurrence are recommended? What is the timeline for implementation?

The recommended solutions should address any necessary improvements needed to physical, technical and administrative safeguards to reduce future breaches.

Answer:

APPENDIX A:

Personal Information and Personal Health Information listing

Note: This is not an exhaustive list of personal information and/or personal health information.

✔	General Personal Information
	name
	address
	phone number
	email address
	date of birth
	age
	gender
	criminal record, status or history
	anyone else's opinions about the individual
	the individual's views or opinions
	religious beliefs or associations
	country of origin
	ethnic or racial origin
	political beliefs or associations
	marital status
	family information or status
	visually recorded information (e.g. photo or video of an individual)
	educational information (status or history)
	employment information (status or history)
	fingerprint
	other

✔	Unique Identifiers
	Social Insurance Number (SIN)
	Driver's Licence Number
	YHCIP# (or other health care number)
	other
✔	**Personal Financial Information**
	credit card number
	bank account number
	income tax information
	financial status or history
	other
✔	**Personal Health Information**
	health care status or history
	test results, medical images
	medications
	diagnosis
	disability
	other

Yukon
Health and Social Services

June 2016