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

Policy No.

TITLE: SAMPLE - Security Breach Policy

EFFECTIVE:

---

1. **SCOPE**

Definitions of key terms are set out in section 1.5 of this policy.

1.1 Authority

Yukon's *Health Information Privacy and Management Act* (*HIPMA*) (Part 3, Division 5, s. 29 to 31).

1.2 Application

This policy and the associated documents apply to all employees of {*Name of Custodian*}

1.3 Purpose

The purpose of this policy is to provide rationale and procedures to identify, contain and notify the affected individuals of real or suspected breaches.

This policy will also allow {*Name of Custodian*} to respond quickly in a coordinated manner, identify roles and responsibilities and the process for an effective response.

1.4 Background

HIPMA establishes rules for the collection, use, disclosure or and access to PHI that protect its confidentiality, privacy, integrity and security. (*Health Information Privacy and Management Act* Part 3 Divisions 1, 3 and 4)

A breach occurs if there is a theft or loss of information or unauthorized disclosure of, or access to, 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
- sharing a story with identifying client information on social media without consent

1.5 Definitions

Health information means identifying information of an individual, in a recorded or unrecorded form that relates to: the individual's health or the provision of health care to them; payments for health care; donation of body parts, tissue or substance of an individual, or that is derived from testing (*Health Information Privacy and Management Act* ss. 2(1))

Personal health information (PHI) means health information of an individual and prescribed registration information and prescribed provider registration information in respect of the individual (*Health Information Privacy and Management Act* ss .2(1))

Confidentiality means the obligation to protect the secrecy of information entrusted to you and not to misuse it.

Privacy means is the right of an individual to control access to his or her information.

Security means the technologies and methods used to protect the confidentiality, integrity and availability of information, both in electronic and paper format, while the information is being used, stored or transferred.

1.6 Principles

- {*Name of Custodian*} must manage personal information in a privacy-protective manner in compliance with *HIPMA*
- An individual's right to protection of personal health information when collected by {*Name of Custodian*}
- {*Name of Custodian*} transparency in how it protects personal health information
- Obligation to provide notification of privacy breach in certain circumstances
- Continuous improvement

2. POLICY STATEMENT

{*Name of Custodian*} takes very seriously its responsibility to protect PHI.

If an employee believes a breach has occurred in relation to PHI, it is considered a breach and the breach must be reported immediately to {*the position title of the individual responsible for responding to breaches*}. (*Health Information Privacy and Management Act* para. 29(a))

The {*the position title of the individual responsible for responding to breaches*} is responsible for following the {*Name of Custodian}* Privacy Breach Protocol (Appendix 1) and completing the Breach Report (Appendix 2).

Appendix 1: Breach Protocol
Appendix 2: Breach Report