Yukon
Health and Social Services

HEALTH AND SOCIAL SERVICES
CORPORATE POLICIES

POLICY IM-007
Form appended

TITLE: Security Breach Policy

CATEGORY: Information Management

EFFECTIVE: August 31, 2016

1.0 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*, s. 29 to 31).

1.2 Application

This policy and the associated documents apply to all employees and agents of Health and Social Services (HSS).

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 of personal health information (PHI) and personal information (PI).

This policy will also allow HSS to respond quickly in a coordinated manner, identify roles and responsibilities, and outline 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 (*HIPMA*, 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*

A breach also occurs if there is a theft or loss of information or unauthorized collection, use or disclosure of, or access to personal information held by the Department.

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
- being overheard discussing PI/PHI of a client in a public setting with someone who does not need to know, or
- sharing a story with identifying client information on social media without consent.

1.5 Definitions

Personal information (PI) means information about an identifiable individual including name, address, telephone number, health care history (physical or mental disability); educational, financial, criminal or employment history; blood type (**Note**: this is not an exhaustive list) (*Access to Information and Protection of Privacy Act,* s.3)

Health information means identifying information of an individual, in a recorded or unrecorded form e.g. individual's health; provision of health care; payments for health care; donation of body parts, tissue or substance of an individual or testing (*HIPMA,* s. 2(1)).

Personal health information (PHI) means health information of an individual and prescribed registration information and provider registry information in respect of an individual (*HIPMA,* s.2 (1)).

Confidentiality means the obligation to protect the secrecy of information entrusted to you and not to misuse it. (For example, Health and Social Services has a duty to protect the personal information/personal health information of individuals with certain communicable diseases, i.e., keep it confidential, even though the individual has no privacy right to stop Health and Social Services from collecting it.)

Privacy means is the right of an individual to control access to his or her information. (Sometimes individuals are not granted this right in law. For

example, it is mandatory to report the relevant personal health information of individuals with certain communicable diseases.)

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. (For example, a home care nurse uses an encrypted laptop to take notes while in her client's home. Encryption is a technology used to scramble electronic information. If her laptop is lost, it is very unlikely anyone could access the information on it. If she has to take paper records, she uses a locked bag or briefcase.)

Privacy Officer mean Manager, Information and Records

1.6 Principles

- HSS must manage personal health information in a privacy-protective manner in compliance with *HIPMA.*
- An individual's rights in relation to the protection of his or her PI/PHI must be respected when such information is collected by the Department.
- Departmental transparency regarding how it protects PI/PHI is consistent with the department's culture of open discussion about risk
- The Department has an obligation to provide notification of breaches in certain circumstances
- Continuous improvement is key to reduce the instances of breaches. Lessons learned from past breaches can help reduce the risk of reoccurrence.

2.0 POLICY STATEMENT

Health and Social Services takes its responsibility to protect PI/PHI very seriously.

If an employee believes a breach has occurred in relation to PI/PHI, it is considered a breach and must be reported immediately to your Supervisor (*HIPMA,* s.29(a)).

The Supervisor and the Department's Privacy Officer is responsible for following this policy and completing the Departmental Breach Report (Appendix 1).

The Department will review and analyze each breach to determine appropriate strategies to prevent the breach from occurring again.

Process for Managing Breaches:

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 the breach is an unauthorized access to an IT asset such as a computer, server or network, you MUST shut down the affected asset and contact your Network Administrator immediately.

If uncertain whether a breach has occurred, contact the Department's Privacy Officer (456-3953).

Step 2: Notify Manager/Supervisor and the Department's Privacy Officer
Recommended Timeline: Same day the breach is discovered.

- All breaches, real or suspected must be reported immediately to the Supervisor.
- The manager or supervisor will notify the affected program's Director and the Department's Privacy Officer.
- The manager or supervisor responsible will begin completing the Departmental Breach Report and answer questions 1.1 and 1.2.
- In collaboration with the Manager/Supervisor, the Department's Privacy Officer will determine who among the Department's executive should be notified. For example, Assistant Deputy Minister responsible, Director of Communications or Deputy Minister.
- The Department's Privacy Officer will assist in determining whether the breach involves one or multiple departments.
- The Director responsible, in discussions with the department's Privacy Officer, will determine who will be the lead in conducting the investigation and completing the Departmental Breach Report.
- If the manager or supervisor believes the breach resulted from criminal activity, notify the RCMP immediately.

Step 3: Determine the risk of harm to affected individuals
Recommended timeline: Within 5 working days after breach was discovered

- The Department's Privacy Officer, or delegate completes section 2 of the Departmental Breach Report.
    - The Department's Privacy Officer may also create a breach response team. A breach response team may include representatives from: legal services branch, IT unit and an individual from the affected program.
- Refer question 2.3 of the Departmental Breach Report, 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 Department's Privacy Officer in consultation with the affected program area will determine whether notification is required or appropriate. Use the parameters outlined in question 2.4 of the Departmental Breach Report, when making this determination.

- **Determination there is a likelihood of significant harm.**
    - If there is a likelihood of significant harm, affected individuals **MUST** be notified (*HIPMA*, s.30(2)).
    - 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

  (*HIPMA*, s.30(3) and 31)

- **Determination there is not a likelihood of significant harm.**
    - If it is determined that there is not a likelihood of significant harm, the department is not obliged to notify affected individuals or the OPIC. However, a mitigation strategy should be developed to prevent similar future breaches.

3.0 ROLES AND RESPONSIBILITIES

Deputy Minister

- Sets the tone that a breach is taken seriously and must be addressed in the most expeditious manner possible;
- Notifies affected individuals of breach, and
- Review and signoff of Breach Report.

Assistant Deputy Ministers

- Reinforce within their portfolios, that a breach is taken seriously and must be addressed in the most expeditious manner possible, and
- Review and signoff of Breach Report.

Directors, Managers and Supervisors

- Ensure employees are aware of this policy;
- Monitor employee compliance with the policy;
- Assigns contact person to assist with breach investigation and breach report;
- Ensure employees participate in training in information privacy management and breach prevention;
- Responsible for notifying their senior management and the Privacy Officer of any breach, and
- Review and signoff of Breach Report.

Privacy Officer

- Leads investigations into breaches and assists with drafting of Breach Report;
- Monitors and tracks privacy breach and provides quarterly report to Assistance Deputy Minister – Corporate Services;
- Develops training and tools for managing privacy and a breach of privacy;
- Ensures the Deputy Minister, Assistant Deputy Minister responsible, Director of Communications, if warranted, are aware of any breaches;
- Develops an on-going communication strategy to raise awareness of privacy, and
- Review and signoff of Breach Report.

All Employees

- Have a legal responsibility for protecting all personal information they collect or have access to;
- Are accountable for adhering to this policy;
- Are responsible for immediately notifying their supervisor of real or suspected breaches, and

- May only collect, use, disclose or access PI/PHI for the purposes of carrying out their specific job function.

4.0 PERFORMANCE REVIEW

- Number of breaches reported
- List of mitigation strategies developed
- Number of Information and Privacy Commissioner investigations

Appendix 1: Departmental Breach Report

VERSION: 1 **DATE APPROVED:** August 31/16

APPROVED BY: _____

Bruce McLennan, Deputy Minister

SPONSOR: Birgitte Hunter, Assistant Deputy Minister – Corporate Services

CONTACT: HSS Privacy Officer

KEYWORDS: Breach, Security Breach

RELATED REFERENCES: *Health Information Privacy and Management Act*, Risk Management Policy (GOV-002), HSS Pledge of Confidentiality

DATE TO BE REVIEWED: September 30, 2017

DATE AMENDED:

Yukon
Health and Social Services

DEPARTMENTAL BREACH REPORT

1. CONTAINMENT OF BREACH

Name of the Branch:	
Reported by:	
Email/Phone:	
Date breach occurred: (YYYY-MM-DD)	
Date breach was discovered: (YYYY-MM-DD)	
Physical location/address of breach:	

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

A breach occurs if there is a theft or loss of information or unauthorized disclosure of, or access to, personal information (PI) or personal health information (PHI) contrary to the *Health Information Privacy and Management Act (HIPMA).*

Some examples of a breach are:

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

Refer to Appendix A of this form for examples of "personal information" and "personal health information".

Example: Bill lost a USB that contained the employee information of ten individuals. The employee information included the following information for each individual: name, date-of-birth, residential address, personal phone number, employee number, employment history and performance evaluations.

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 containment actions are:

- *Immediately recovering the information and have the 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 electronic system that was breached;*
- *Revoking or changing computer access code; or*
- *Contacting the Health and Social Services Privacy Officer.*

Refer to Appendix A of this form for examples of "personal information" and "personal health information".

Example: When Bill realised the USB was missing, he took the following steps: He immediately contacted his privacy officer and tried to locate the lost USB. Bill retraced his steps; he searched his office and his car. He then contacted the government office where he brought the USB. To Bill's relief, his colleague confirmed he was in possession of the USB.

Next, Bill immediately retrieved the USB from his colleague. Unfortunately, Bill's colleague confirmed he had accessed the contents of the USB. Bill then had his colleague confirm, in writing, that no copies of the USB were made and the information he viewed will not be communicated.

Answer:

CONTACT THE DEPARTMENT'S PRIVACY OFFICER BEFORE PROCEDING TO THE FOLLOWING SECTIONS OF THE REPORT

2. RISK OF HARM

Note: Health and Social Services Privacy Officer or delegate should complete the following section.

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?*

Example: Bill, along with his Privacy Officer, determined the breach was caused by the loss of an unencrypted USB. Because the USB was recovered within hours of Bill misplacing the USB, it was determined there was no risk of further exposure of the information.

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 affect (≥50)*
- *Numbers are not known?*

Example: Bill determined that an identified and limited group of ten individuals are affected.

Answer:

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

Part 1- Determine the Sensitivity of the Information

Privacy Commissioners have held the following types of information to be highly sensitive: SIN, date-of-birth, driver's license number, credit card numbers, signatures, medical information (psychiatric or addiction counselling notes, for example), employee information (poor performance or termination information, for example).

Commissioners have held the following types of information to be low or moderately sensitive: Names, phone numbers, email addresses, and bank accounts.

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.

Example: Bill determined that the lost information included highly sensitive information. It included employee information, including personnel evaluations, as well as the name, date-of-birth, and address of individuals.

Next, because the information included employee information, Bill determined that there is a risk of humiliation and damage to the reputation of the affected individuals. Bill also determined there is a risk of identity theft as individuals' name, date-of-birth, and address were included together. Further, Bill determined there is a risk to the organization as employee trust could be undermined around how the organization handles their employee information.

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 was 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 fraud;* • *The number of 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 Yukon.); and* • *The immediate containment measures taken?* ***Example: Bill determined that there was a low likelihood of significant harm. Bill immediately noticed the USB was missing upon returning to his office and promptly located it. Further, Bill received written confirmation that the USB was not copied or communicated. Finally, Bill confirmed that his colleague did not know any of the individuals' information he accessed.*** ***As a result, Bill is not required to notify the affected individuals, nor the Office of the Information and Privacy Commissioner.***
Answer:

Note: If you determine there is a likelihood of significant harm, you must notify the affected individuals as well as the Office of the Information and Privacy Commissioner.

3. NOTIFICATION

3.1 Internal Notifications:

Has the Director of the affected program area been notified?	
Has the Assistant Deputy Minister of the affected program been notified?	
Has the Deputy Minister been notified?	
Has Legal Services Branch of the Department of Justice been notified?	
Have the RCMP been notified, if necessary?	

3.2 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 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 have been taken to reduce the risk of harm to the individual as a result of the breach;*
- *Identify who can be contacted within your organization with questions; and*
- *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: Use of YG firewall, 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 (PI)

- 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
- type of service received

Unique Identifiers

- Social Insurance Number (SIN)
- Driver's Licence Number
- Yukon Health Care Insurance Plan number (or other health care number)

Personal Financial Information

- credit card number
- bank account number
- income tax information
- financial status or history

Personal Health Information (PHI)

- Yukon Health Care Insurance Plan number
- health care status or history
- test results, medical images
- medications
- diagnosis
- disability