



MAY 31 2017

Ms. Sue Cullen  
Chief Executive Officer  
Northwest Territories Health and Social Services Authority  
PO BOX 1320  
YELLOWKNIFE NT X1A 2L9

Ms. Erin Griffiths  
Chief Executive Officer  
Hay River Health and Social Services Authority  
37911 MACKENZIE HIGHWAY  
HAY RIVER NT X0E 0R6

Mr. Kevin Armstrong  
Chief Executive Officer  
Tłıchǫ Community Services Agency  
P.O. BOX 412  
BEHCHOKǾ, NT X0E 0Y0

Dear Chief Executive Officers:

**Privacy Standards, Policies and Procedures – Ministerial Directive**

Please find attached a signed Ministerial Directive and associated Privacy Standards, Policies and Procedures. The Directive requires that the Department of Health and Social Services (DHSS) and Health and Social Services Authorities (HSSAs) follow the approved standards, policies and procedures referred to in this Directive.

As you know, the *Health Information Act* (HIA) has been in force since October 2015. Both the Information Privacy Commissioner and legal counsel have recommended that to fully meet the requirements of the HIA, the adoption of standards, policies and procedures is necessary. In order to ensure that there are consistent standards, policies and procedures across the

.../2

system, the DHSS has developed the attached for your use. It is important to remember that most of these policies are not specific to only health information, and should be applied to any information that is collected, used and disclosed across the health and social system unless otherwise specified.

While it is understood that there may be some technical issues with complying with all of the provisions in some of the policies, such as the Masking Policy for example, we are circulating the policy framework now to guide your work in this area.

Please note that the Ministerial Directive 2009-01 signed January 29, 2009 is rescinded as it was issued before the HIA came into force. A formal rescinding document signed by the Minister will be forthcoming.

If you have any questions, please contact Ms. Dana Webster, A/Chief Health Privacy Officer at 867-767- 9052 ext. 49040.

Sincerely,



Debbie DeLancey  
Deputy Minister  
Health and Social Services

Attachment

c Ms. Dana Webster  
A/Chief Health Privacy Officer  
Department of Health and Social Services

Ms. Michele Herriot  
Chief Information Officer  
Department of Health and Social Services

Mr. Gary Toft  
Director, Policy Legislation and Communications  
Department of Health and Social Services

# Health and Social Services Consent Conditions Policy

---

## Policy Statement

A consistent process is necessary across the health and social services system to respect, acknowledge, follow, and appropriately document consent conditions requested by individuals or substitute decision makers.

## Scope

This Policy applies to all consent conditions received by employees of the Department of Health and Social Services (Department) and Health and Social Services Authorities (HSSAs).

Conditions placed on consent do not apply when the information is required by law or by established institutional or professional practice standards.

## Definitions

The following terms apply to this Policy:

“Consent Condition” includes an express instruction and refers to a limit, set by an individual or substitute decision maker, on how the Department/HSSAs may collect, use or disclose personal health information about the individual.

“Employee” for the purpose of this Policy means all individuals employed by the Department or HSSA including salaried, contracted or locum health practitioners and individuals whose positions are federally funded.

“Express instructions” are specific directions provided by an individual or substitute decision maker about how the individual’s personal health information may or may not be, collected, used or disclosed that must be clearly documented on the individual’s record so that anyone who accesses the record will be aware of them.

“Established institutional practice standards” means a practice which guides the Department/HSSA’s behavior, i.e. Accreditation Canada Guidelines, Ministerial Directives, any policies, procedures, guidelines, and standards adopted/established by the Department/HSSAs.

“Established professional practice standards” means a practice that sets out the professional basis for practice and standards of practice, i.e. code of ethics that is recognized, adopted, or established by professional licensing bodies or Canadian professional associations.

“Health and Social Services Authorities” refers to the Northwest Territories Health and Social Services Authority and Boards of Management under the *Hospital Insurance and the Health and Social Services Administration Act*.

“Personal health information” means information in any form that identifies an individual, or in respect of which it is reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual:

- (a) information about the health and health care history of an individual,
- (b) information respecting health services provided to an individual,
- (c) information about eligibility or registration of an individual for a health service or related product or benefit,
- (d) information about the payment for a health service for an individual,
- (e) information collected in the course of providing a health service to an individual or information that is collected incidentally to the provision of a health service to an individual, including the individual's name and contact information,
- (f) a personal health number, other identifying number, symbol, or other particular assigned to an individual in respect of health services or health information,
- (g) prescribed information about a health service provider that provides a health service to an individual,
- (h) information respecting the donation by an individual of a body part or bodily substance,
- (i) information prescribed as personal health information in the Health Information Regulations.

“Substitute decision maker” means a person, recognized under the *Health Information Act* who is:

- (a) the individual's guardian or parent or person with lawful custody, if the individual is under 19 and is not a mature minor,
- (b) the individual's guardian, trustee, or legal representative,
- (c) a person who holds the individual's power of attorney or the person named in a personal directive,
- (d) anyone authorized in writing by the individual when the individual was mentally competent,
- (e) a deceased individual's personal representative, estate executor, or spouse,
- (f) a deceased individual's relative or an adult who had a close personal relationship with the individual,



- (g) a deceased individual's substitute decision-maker identified by the *Human Tissue Donation Act*,
- (h) a prescribed person in prescribed circumstances and who:
  - i. makes decisions on behalf of an individual about their personal health information, **while**
  - ii. considering the individual's wishes and beliefs, **and**
  - iii. assessing the benefits against the risks before making a decision.

## Provisions

- 1) The Department/HSSAs must:
  - a. take reasonable steps to fully comply with valid consent conditions, as specified in the provisions below;
  - b. track and document consent conditions that are in place; and,
  - c. identify and authorize employees to process consent condition requests.
- 2) Consent conditions may only apply to the future collection, use, or disclosure of an individual's personal health information.
- 3) Consent conditions must only be requested by the individual the information is about or the individual's substitute decision maker.
- 4) Consent condition requests may be received:
  - a. in written form; or,
  - b. in verbal form when it is impractical for an individual/substitute decision maker to write them.
- 5) Employees authorized to process consent conditions must:
  - a. acknowledge receipt of the consent conditions and express instructions in writing;
  - b. review the consent conditions and express instructions with the individual;
  - c. respond to the individual's consent conditions request;
  - d. document and record any received consent conditions;
    - i. if consent conditions are received in verbal form, a record must contain an explanation from the individual of why it was impractical to provide consent conditions in writing, along with the date and signature of the authorized employee.
  - e. inform the individual of the implications of making such a condition, if there are any, and how their consent conditions may impact their health care;
  - f. clarify with the individual the parameters of their consent conditions and express instructions;

- g. advise the individual if the Department/HSSAs are unable to meet part or all of their conditions;
  - h. discuss with the individual options available of how the Department/HSSAs can accommodate their consent conditions;
  - i. review the consent conditions and express instructions with the individual;
  - j. create a final version of the consent conditions in agreement;
  - k. provide a copy of the signed final version of the consent conditions to the individual;
  - l. keep a record of the individual's final consent conditions including express instructions; and,
  - m. work with necessary persons to implement consent conditions.
- 6) Once a consent condition has been implemented, the Department/HSSAs must take reasonable steps to give notice of the condition to any person or organization to which the Department/HSSA discloses information.
- 7) If the Department, HSSA or a health service provider discloses limited personal health information to a health service provider based on a consent condition, and he/she feels that the information not disclosed may affect the care of the patient, they must give notice to the health care provider that
  - a. the shared information is limited because of a consent condition; and,
  - b. they consider the undisclosed information to be necessary to provide best care to the individual.
- 8) Consent conditions remain in effect in many circumstances, including but not limited to:
  - a. after the individual's death;
  - b. when providing further health services to the individual, verifying eligibility of that individual for a health service, and when disclosing information for continued care;
  - c. when disclosing information about the individual who is injured, ill or incapacitated to contact a person who has a close personal relationship with the individual or a potential substitute decision maker;
  - d. when disclosing person health information about the individual when a patient in a health facility or resident to another person who has a close personal relationship with the individual; or,
  - e. until an individual or substitute decision maker:
    - i. makes changes to the current consent conditions; or,
    - ii. revokes the current consent conditions.

- 9) Consent conditions do not apply in some circumstances, including but not limited to:
- a. statistical, non-identifiable and de-identified information;
  - b. situations where the Department/HSSAs are allowed to collect, use or share information about an individual without their consent, including but not limited to:
    - i. disclosure to law enforcement;
    - ii. disclosure to a correctional facility;
    - iii. disclosure to another facility in which an individual is lawfully detained
    - iv. disclosure to identify a deceased individual;
    - v. disclosure for the prevention of harm to an individual or the public; or,
    - vi. disclosure for audit, legal services, or risk management.

## Authority and References

*Health Information Act*

Ministerial Directive 2016-01: Privacy Standards, Policies and Standards

De-identification Policy

Masking Policy

Withdrawing Consent Policy

Disclosure of Information to Officials in Official Capacity Policy

  
\_\_\_\_\_  
Deputy Minister

  
\_\_\_\_\_  
Date

# Health and Social Services Contractor Compliance Policy

---

## Policy Statement

Reasonable measures must be taken to ensure that personal and personal health information are protected when a contractor is used to provide a service on behalf of the Department of Health and Social Services (Department) or Health and Social Services Authorities (HSSAs).

## Scope

This Policy applies to:

- 1) All employees working for the Department and HSSAs who hire contractors to do work that involves personal or personal health information.
- 2) Individuals who are under contract to provide services.

## Definitions

The following terms apply to this Policy:

“Employee” for the purpose of this Policy means all individuals employed by the Department or HSSA including salaried, contracted or locum health practitioners and individuals whose positions are federally funded.

“Health and Social Services Authorities” refers to the Northwest Territories Health and Social Services Authority and Boards of Management under the *Hospital Insurance and Health and Social Services Administration Act*.

“Personal information” means information about an identifiable individual, including

- (a) the individual's name, home or business address or home or business telephone number,
- (b) the individual's race, colour, national or ethnic origin or religious or political beliefs or associations,
- (c) the individual's age, sex, sexual orientation, marital status or family status,
- (d) an identifying number, symbol or other particular assigned to the individual,
- (e) the individual's fingerprints, blood type or inheritable characteristics,
- (f) information about the individual's health and health care history, including information about a physical or mental disability,

- (g) information about the individual's educational, financial, criminal or employment history,
- (h) anyone else's opinions about the individual,
- (i) the individual's personal opinions, except where they are about someone else.

"Personal health information" means information in any form that identifies an individual, or in respect of which it is reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual:

- (a) information about the health and health care history of an individual,
- (b) information respecting health services provided to an individual,
- (c) information about eligibility or registration of an individual for a health service or related product or benefit,
- (d) information about the payment for a health service for an individual,
- (e) information collected in the course of providing a health service to an individual or information that is collected incidentally to the provision of a health service to an individual, including the individual's name and contact information,
- (f) a personal health number, other identifying number, symbol, or other particular assigned to an individual in respect of health services or health information,
- (g) prescribed information about a health service provider that provides a health service to an individual,
- (h) information respecting the donation by an individual of a body part or bodily substance,
- (i) information prescribed as personal health information in the Health Information Regulations.

## Provisions

- 1) The Department and HSSAs **must** take reasonable steps to ensure that its contractors comply with the *Health Information Act* (HIA) and its regulations and/or the *Access to Information Protection of Privacy Act* and its regulations, as applicable.
- 2) The following are reasonable steps that must be taken:
  - a. The Department/HSSAs may only allow its contractors to collect, use and disclose personal and/or personal health information if:
    - i. The Department/HSSAs may collect, use and disclose the personal and/or personal health information.
    - ii. Contractors will collect, use and disclose the information as part of their responsibilities outlined in the service contract

- and their actions are not contrary to the limits imposed by the Department/HSSA, HIA or another law.
- b. The Department/HSSAs should consider the following when developing a service contract:
- i. Define unique, specific terms that are used throughout the contract.
  - ii. Include a clause that requires the contractor to abide by the HIA and/or ATIPP.
  - iii. Describe what personal and/or personal health information will be shared, why it is being shared, and how it will be shared.
  - iv. Identify how the shared information will be used and require the contractor to use the information for only those purposes.
  - v. Identify whether any information may be linked to or matched with other information.
  - vi. Place restrictions on disclosure as necessary.
  - vii. Include the timeframe that personal and/or personal health information will be kept and how it will be disposed of or returned.
  - viii. Set out the safeguards (administrative, physical and technical) needed to protect the information and what must occur if a privacy breach is suspected.
  - ix. Limit the contract term to ensure that information will only be shared for as long as necessary.
- c. **Contractors must:**
- i. Have the Department's/HSSA's permission to collect, use and disclose personal and/ or personal health information on the Department's/HSSA's behalf.
  - ii. Use information only for the identified purpose, except if allowed and/or required by HIA or other law.
  - iii. Notify the Department/HSSA if the information they handle has been associated with breach activity as soon as reasonably possible.
  - iv. Collect, use and disclose the least possible personal and/or personal health information and only on a need-to-know basis.
  - v. Collect, use and disclose de-identified information unless identifiable information is necessary.
  - vi. Follow privacy and security safeguard measures developed by the Department/HSSA, and as well as set in their contract.
  - vii. Provide the Department/HSSA with their privacy and security policies, procedures and safeguard measures they follow prior to receiving personal and/or personal health information.

1. If contractors do not have privacy and security policies, procedures and safeguard measures, or they do not align with the Department/HSSA policies and procedures, contractors must complete the appropriate level of mandatory training in accordance with the Mandatory Training Policy.
- viii. Be provided with a copy of all applicable Department/HSSA privacy standards, policies and procedures and guidelines.
- ix. Upon request, provide the Department/HSSA with a Privacy Impact Assessment(s) for any information system and/or communications technology for which contractor is primarily responsible that will be used to store, manage or transfer personal and/or personal health information as a part of the contracted services.
- x. Have privacy and security safeguard measures in place that are proportionate to privacy risks.

## Authority and References

*Access to Information and Protection of Privacy Act*

*Health Information Act*

Ministerial Directive 2016-02: Privacy Standards, Policies and Standards

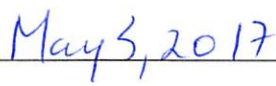
Privacy Impact Assessment Policy

Mandatory Training Policy

Privacy Breach Policy

Electronically Stored and Transferred Information Policy

  
\_\_\_\_\_  
Deputy Minister

  
\_\_\_\_\_  
Date

# Health and Social Services De-Identification Policy

---

## Policy Statement

A consistent approach must be used across the health and social services system when applying de-identification methods to comply with safeguard requirements and ensure personal health information is protected.

## Scope

This Policy applies to all employees of the Department of Health and Social Services (Department) and the Health and Social Services Authorities (HSSAs) who are tasked with de-identification.

## Definitions

The following terms apply to this Policy:

“De-identification” refers to the process of manipulating personal health information so that the identity of the individual(s) the information is about cannot reasonably be determined.

“Employees” for the purpose of this Policy means all individuals employed by the Department or HSSA including information managers.

“Health and Social Services Authorities” refers to the Northwest Territories Health and Social Services Authority and Boards of Management under the *Hospital Insurance and the Health and Social Services Administration Act*.

“Information manager” means a person or organization that provides one or more of the following services for the Department of HSSA:

- (a) the processing, storage, retrieval or disposal of personal health information,
- (b) the transforming of personal health information, including the transforming of person health information to create or produce non-identifying information,
- (c) information management services, information system services or technology services.

“Manipulating” refers to, stripping, encoding or otherwise transforming personal health information in the context of personal health information.



“Non-identifying information” refers to personal health information that cannot be reasonably used to determine an individual’s identity or lead to re-identification.

“Personal health information” means information in any form that identifies an individual, or in respect of which it is reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual:

- (a) information about the health and health care history of an individual,
- (b) information respecting health services provided to an individual,
- (c) information about eligibility or registration of an individual for a health service or related product or benefit,
- (d) information about the payment for a health service for an individual,
- (e) information collected in the course of providing a health service to an individual or information that is collected incidentally to the provision of a health service to an individual, including the individual’s name and contact information,
- (f) a personal health number, other identifying number, symbol, or other particular assigned to an individual in respect of health services or health information,
- (g) prescribed information about a health service provider that provides a health service to an individual,
- (h) information respecting the donation by an individual of a body part or bodily substance,
- (i) information prescribed as personal health information in the Health Information Regulations.

“Re-identification” means the process of manipulating previously de-identified personal health information so that the information can reasonably identify an individual or individuals the information is about.

## **Provisions**

- 1) The Department/HSSAs must
  - a. take measures to protect personal health information when applying de-identification methods; and,
  - b. ensure de-identification methods performed by employees meet the standards and best practices as set out in the Personal Health Information De-Identification Guidelines (Appendix 1), as amended from time to time.
- 2) De-identification methods may only be applied by authorized employees, identified by the Department or HSSAs.


- 3) The DHSS Process for Personal Health Information De-Identification (Appendix 1) must be followed when applying de-identification methods.
- 4) Authorized employees must consider the following when determining the appropriate methods of de-identification:
  - a. who may access the de-identified information;
  - b. why the de-identified information may be accessed, and,
  - c. the risk of re-identification, including consideration of whether there is other information available that could lead to re-identification.

## Authority and References

*Access to Information and Protection of Privacy Act*

*Health Information Act*

Ministerial Directive 2016-02: Privacy Standards, Policies and Standards

  
\_\_\_\_\_  
Deputy Minister

*May 3, 2017*  
\_\_\_\_\_  
Date

## Personal Health Information De-Identification Guidelines

As employees of the Health and Social Services system, it is an obligation to ensure we protect client information when using health data and in particular when applying de-identification methods.

The Department has developed these guidelines<sup>1</sup>, to assist Department and HSSAs employees in:

- applying appropriate de-identification methods
- assessing the risk of re-identification.

### Definitions

"Aggregate-level data" means data collected at the record-level then have been averaged or grouped into ranges and reported as a sum to ensure there are no directly identifying variables.

"De-identification" means the process of manipulating personal health information so that the identity of the individual or individuals the information is about cannot reasonably be determined, making the information de-identified health information, the use of which either alone or with other available information cannot reasonably lead to re-identification.

"Record-level data" means data at the level of an individual person.

"Re-identification" means the process of manipulating previously de-identified health information so that the information can reasonably identify an individual or individuals the information is about.

### Applying de-identification methods

Before you apply any de-identification method:

- Be aware of de-identification principles which include:
  - Disclosures are made with the minimum amount of data.
  - A number of de-identification methods are commonly used and available for application (see *Recommended de-identification methods*).
  - No single method can independently meet the diverse needs of de-identifying personal health information.
  - Each de-identification project or file requires a unique process in terms of type of de-identification method to be applied and combination of methods.
- Be capable of applying current de-identification tools and understand the statutory requirements related to de-identification.

To choose an appropriate de-identification method:

- Review the de-identification request and decide which level of data to be released – record-level vs. aggregate data. Record-level data are more prone to re-identification than are aggregate data.
- Decide which method(s) is most appropriate. Data reduction methods are more commonly used than data modification. Data modification methods involve more radical approaches to the data and have greater potential to reduce the informativity of the data.
- Begin with *Reduction in Detail* method followed by *Suppression*. These are:
  - the most accepted methods in practice,
  - the least expensive to apply,
  - the easiest to understand, and
  - the easiest to predict re-identification risk.
- When you apply the pseudonymization method, ensure the generated pseudonyms are specific to a

<sup>1</sup> These guidelines have been developed with permission to use and adopt information from *Pan-Canadian De-identification Guidelines*, produced for the Office of the Privacy Commissioner of Canada, April 2007, the *Tools for De-identification of Personal Health Information* prepared for the Pan Canadian Health Information Privacy Group, September 2009, and the *Best Practice Guidelines for Managing the Disclosure of De-identified Health Information*, produced for the Canadian Institute for Health Information, October 2010.

given data set. It protects control of the data and future capability of data linkage, if needed.

### Assessing re-identification risk levels

The purpose of risk assessment is to determine how much de-identification to perform in order to reduce the risk of re-identification to an acceptable level. (See *Dependency Table*)

The assessment of re-identification risk levels may include:

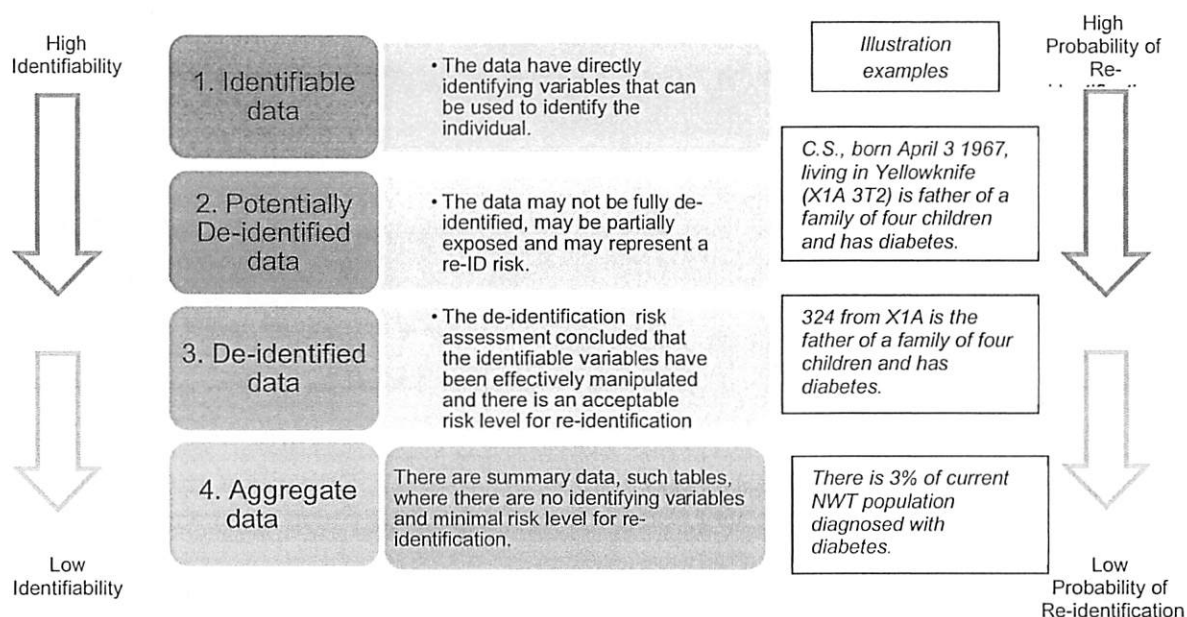
- Map the risk level of re-identification in order to ensure appropriate de-identification methods application. Refer to *2011 CiHi Best Practice Guidelines for Managing the Disclosure of the De-Identified Health Information* and *2007 Pan-Canadian De-Identification Guidelines* documents for further assistance.
- Assess intention and capacity to re-identify; mitigating controls, estimate probability of a re-identification attempt, estimate how much de-identification is required.
- Consider establishing flexible guidelines for acceptable levels of re-identification risk that can address a range of re-identification risk scenarios.

The risk of re-identification may shift as technologies develop and a larger amount of information is available. Re-assessment of the re-identification risk levels on a regular basis is advised, and may include:

- Assess if higher level of de-identification is needed;
- Assess if a release of additional de-identified information could potentially assist in the re-identification of already available information.
- Assess the features of the analytics reporting in e-systems when querying an e-system.

### Dependency Table

#### Identifiability and Probability of re-identification based on different types of data



## Recommended de-identification methods

De-identification methods		Application		
		Geo-Code	Numeric	Alphanumeric
Data Reduction	<b>Reduction in Detail</b> Involves reduction in the detail of the data through rounding or collapsing the data values into larger categories.	Reduce postal codes to first 3 characters, i.e. Forward Sortation Area.	Round birth dates to year. Express dates relative to a milestone date.	
	<b>Suppression</b> Involves the removal or withholding of the data records.	As a rule of thumb, suppress geo-codes when they contain six observations or less.	As a rule of thumb, suppress numbers when they contain six observations or less.	As a rule of thumb, suppress alpha variables when they contain six observations or less.
	<b>Sampling</b> Involves random samples of the records from a database.	E.g. Database contains too many records for analysis. If analysis was conducted using a random sample of one-fifth of the records from a database and additional technique was applied (e.g. reduction in detail). Sampling is often used in combination with other techniques, rather than on its own to protect against risk of re-identification.		
Data Modification	<b>Random addition of 'noise'</b> Involves adding random 'noise' to the values of data in order to disguise its true value.	Randomly change the actual postal codes within certain pre-determined acceptable range (e.g. first or last two)	Randomly change the actual date of birth within certain pre-determined acceptable range (e.g. 6 months)	Randomly change the name within certain pre-determined acceptable range (e.g. first or last)
	<b>Data swapping</b> Involves identification of records of pairs of individuals with roughly the same characteristics and the data values are then swapped between the two records.	De-identified personal health information is created with records that are no longer the original records, but the analysis produces same results as achieved using original personal health information.		
	<b>Substitution</b> Removes the association between the individual and the identifying data by replacing original data with random or exchanged values.	If postal code is manipulated then ensure telephone area code is consistent.	If health card number is manipulated then ensure the new number can pass a checksum validation check.	Select new names in same proportion as in general public If surname is manipulated then ensure the new name has the same number of characters and ethnicity.
	<b>Pseudonymization</b> Removes the association between the individual and the identifying data by replacing the data with one or more pseudonyms (aka codes).	Can be applied to most geo- data.	Can be applied to most numeric data. Date of birth (and/or name) can be replaced with a unique pseudonym. Pseudonyms should be independently generated.	Can be applied to most alpha data. To facilitate linkages across databases, the pseudonym generated for the same individual must be consistent.

# Health and Social Services

## Electronically Stored and Transferred Information Policy

---

### Policy Statement

A consistent approach is needed to ensure safe and secure storage and transfer of electronic information.

### Scope

This Policy applies to:

- 1) All employees, volunteers, contractors and information managers of the Department of Health and Social Services and the Health and Social Services Authorities (HSSAs) when storing and transferring personal, personal health and confidential information in electronic format on any portable devices, including but not limited to:
  - Laptops
  - USB flash drives (USB keys, memory sticks, jump drives, thumb drives)
  - Portable external hard drives
  - Tablets (iPads, Galaxy Tab)
  - Smartphones (iPhone, BlackBerry)
  - MP3 players (iPod)
  - Electronic pen (E-pen)

### Definitions

The following terms apply to this Policy:

“Confidential information” is non-public information that is only shared with a limited number of individuals for a specific purpose. Examples of confidential information include, but are not limited to:

- Personal information about clients (such as child protection, adoption, medical records, documents obtained for public health surveillance purposes, etc.)
- Personal information about employees (such as performance appraisals, medical notes, labour relations documentation, etc.)
- Legal opinions
- Decision papers and other material intended for Cabinet or the Financial Management Board
- Any information that, if disclosed, may result in harm to the Government of the Northwest Territories (GNWT) or other interests.

"Electronically" means anything created, recorded, transmitted or stored in digital form or in other intangible form by electronic, magnetic, optical or other similar means.

"Employee" for the purpose of this Policy means all individuals employed by the Department or HSSA including salaried, contracted or locum health practitioners and individuals whose positions are federally funded.

"Health and Social Services Authorities" refers to the Northwest Territories Health and Social Services Authority and Boards of Management under the *Hospital Insurance and Health and Social Services Administration Act*.

"Information manager" means a person or organization that provides one or more of the following services for the Department of HSSA:

- (a) the processing, storage, retrieval or disposal of personal health information,
- (b) the transforming of personal health information, including the transforming of person health information to create or produce non-identifying information,
- (c) information management services, information system services or technology services.

"Personal information" means information about an identifiable individual, including

- (a) the individual's name, home or business address or home or business telephone number,
- (b) the individual's race, colour, national or ethnic origin or religious or political beliefs or associations,
- (c) the individual's age, sex, sexual orientation, marital status or family status,
- (d) an identifying number, symbol or other particular assigned to the individual,
- (e) the individual's fingerprints, blood type or inheritable characteristics,
- (f) information about the individual's health and health care history, including information about a physical or mental disability,
- (g) information about the individual's educational, financial, criminal or employment history,
- (h) anyone else's opinions about the individual,
- (i) the individual's personal opinions, except where they are about someone else.

"Personal health information" means information in any form that identifies an individual, or in respect of which it is reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual:

- (a) information about the health and health care history of an individual,
- (b) information respecting health services provided to an individual,

- (c) information about eligibility or registration of an individual for a health service or related product or benefit,
- (d) information about the payment for a health service for an individual,
- (e) information collected in the course of providing a health service to an individual or information that is collected incidentally to the provision of a health service to an individual, including the individual's name and contact information,
- (f) a personal health number, other identifying number, symbol, or other particular assigned to an individual in respect of health services or health information,
- (g) prescribed information about a health service provider that provides a health service to an individual,
- (h) information respecting the donation by an individual of a body part or bodily substance,
- (i) information prescribed as personal health information in the Health Information Regulations.

"Portable devices" means any type of portable storage device that allows for the storing and transferring of information such as laptops, and USB-based removable media attached to a computer/laptop through a USB connection, such as a flash drive and external hard drive.

## **Provisions**

The following processes must be followed to protect the privacy and security of personal, personal health and confidential information when storing and transferring information in electronic format on portable devices.

### **1) Storage**

- a) Electronically stored information must be kept in a manner that preserves its form and keeps its structure and content intact.
  - Store electronic information in its original version and avoid manipulation unless necessary.
- b) Protect electronically stored information against loss, unauthorized access, manipulation, destruction or theft.
  - Use only secure network drives for storage.
  - Store current or frequently referenced information in a way that allows efficient and authorized access.
  - Limit access to electronic information to only those entitled to it to perform their work.
  - Local backups of electronically stored information must be performed regularly.



2) Transfer

- a) Whenever personal, personal health, and confidential information is electronically transferred it must be appropriately encrypted and/or password-protected to protect the information and prevent unauthorized access during transfer.
- b) Reusable portable devices, such as USB keys or E-pen, must be securely erased when transfer of information is complete.

3) Portable Devices

- a) The transfer and storage of information using a portable device must be restricted and should only be used when absolutely necessary.
- b) When information must be stored or transferred using a portable device:
  - the amount of information stored or transferred must be minimal;
  - Information stored must be removed as soon as possible from the device and saved onto a secure network drive;
  - whenever possible, information transferred using a portable device should be done so over a secure network.

4) Security

- a) Whenever a portable device is not in use, it must be stored securely in a safe locked area (e.g. USB key in a locked cabinet).
- b) Any unattended portable device, such as a laptop, must be logged-off and automatic log-out mechanisms should always be used to prevent unauthorized access.
- c) Any unusual and suspicious events associated with electronically stored and transferred information that may lead to a privacy or security breach must be reported to the supervisor and/or *Health Information Act* (HIA) designated contact person.
- d) Awareness training about electronic information security (including storage, transfer and portable device use) should be maintained and regularly offered.
- e) Security standards established by the Office of the Chief Information Officer must be met.

## Authority and References

*Access to Information and Protection of Privacy Act*

*Electronic Transactions Act*

*Health Information Act*

Ministerial Directive 2016-02: Privacy Standards, Policies and Standards

Privacy Breach Policy

  
\_\_\_\_\_  
Deputy Minister  
\_\_\_\_\_  
Date May 3, 2017

# Health and Social Services Mandatory Training Policy

---

## Policy Statement

Mandatory training with consistent messaging is necessary to ensure that the concepts of confidentiality and privacy are clearly understood by all those who work in and for the health and social services system.

## Scope

This Policy applies to:

- 1) All employees of the Department of Health and Social Services (Department) and the Health and Social Services Authorities (HSSAs).
- 2) Volunteers, contractors and information managers of the Department and HSSAs who may access confidential, personal and/or personal health information.

## Definitions

The following terms apply to this Policy:

“Confidential information” is non-public information that is only shared with a limited number of individuals for a specific purpose. Examples of confidential information include, but are not limited to:

- Personal information about clients (such as child protection, adoption, medical records, documents obtained for public health surveillance purposes, etc.)
- Personal information about employees (such as performance appraisals, medical notes, labour relations documentation, etc.)
- Legal opinions
- Decision papers and other material intended for Cabinet or the Financial Management Board
- Any information that, if disclosed, may result in harm to the Government of the Northwest Territories (GNWT) or other interests.

“Employee” for the purpose of this Policy means all individuals employed by the Department or HSSA including salaried, contracted or locum health practitioners and individuals whose positions are federally funded.

"Health and Social Services Authorities" refers to the Northwest Territories Health and Social Services Authority and Boards of Management under the *Hospital Insurance and the Health and Social Services Administration Act*.

"Information manager" means a person or organization that provides one or more of the following services for the Department of HSSA:

- (a) the processing, storage, retrieval or disposal of personal health information,
- (b) the transforming of personal health information, including the transforming of person health information to create or produce non-identifying information,
- (c) information management services, information system services or technology services.

"Personal information" means information about an identifiable individual, including

- (a) the individual's name, home or business address or home or business telephone number,
- (b) the individual's race, colour, national or ethnic origin or religious or political beliefs or associations,
- (c) the individual's age, sex, sexual orientation, marital status or family status,
- (d) an identifying number, symbol or other particular assigned to the individual,
- (e) the individual's fingerprints, blood type or inheritable characteristics,
- (f) information about the individual's health and health care history, including information about a physical or mental disability,
- (g) information about the individual's educational, financial, criminal or employment history,
- (h) anyone else's opinions about the individual,
- (i) the individual's personal opinions, except where they are about someone else.

"Personal health information" means information in any form that identifies an individual, or in respect of which it is reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual:

- (a) information about the health and health care history of an individual,
- (b) information respecting health services provided to an individual,
- (c) information about eligibility or registration of an individual for a health service or related product or benefit,
- (d) information about the payment for a health service for an individual,
- (e) information collected in the course of providing a health service to an individual or information that is collected incidentally to the provision of a health service to an individual, including the individual's name and contact information,

- (f) a personal health number, other identifying number, symbol, or other particular assigned to an individual in respect of health services or health information,
- (g) prescribed information about a health service provider that provides a health service to an individual,
- (h) information respecting the donation by an individual of a body part or bodily substance,
- (i) information prescribed as personal health information in the Health Information Regulations.

## Provisions

- 1) Immediate supervisors must ensure employees, contractors, volunteers and information managers complete the appropriate level of mandatory training in accordance with Appendix 1.
- 2) Specific training material developed by the Department must be used.
- 3) Mandatory training must be completed:
  - a. Within 3 months of the employee's start date
    - i. for new employees
    - ii. for returning employees with no privacy training in the past year
  - b. Annually
    - i. for all employees, contractors, volunteers and information managers.
- 4) Completed mandatory training must be tracked and documented:
  - a. The employee's immediate supervisor must keep a record of training attendance.
  - b. The Department and HSSAs must also maintain a central record of attendance for the training of all employees, contractors, volunteers and information managers.
- 5) Requirement to obtain specific training to comply with confidentiality and privacy provisions under the *Child and Family Services Act* and *Mental Health Act*, and specific e-system application training, continue to apply notwithstanding this Policy.

## Exception

This Policy does not apply to contractors and information managers if their privacy and security policies, procedures and safeguard measures align with the Department and HSSA policies and procedures.

## Authority and References

*Access to Information and Protection of Privacy Act*

*Child and Family Services Act*

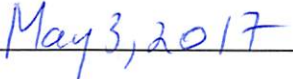
*Health Information Act*

*Mental Health Act*

Ministerial Directive 2016-02: Privacy Standards, Policies and Standards

Contractor Compliance Policy

  
\_\_\_\_\_  
Deputy Minister

  
\_\_\_\_\_  
Date



## Privacy & Confidentiality Training Modules Overview by Job Area

Mandatory
Mandatory Duties Dependent
Optional

JOB AREA with Information Handling	Handling general information ONLY ( <u>not</u> handling personal and/or personal health information)	Handling personal information	Using electronic information system(s) with personal information	Handling personal health information	Using electronic health information system(s)	Records management / access request processing	Quality Risk Management	Responsible for HIA legislative compliance
TRAINING MODULES	General Privacy and Confidentiality	General Privacy and Confidentiality	General Privacy and Confidentiality	General Privacy and Confidentiality	General Privacy and Confidentiality	General Privacy and Confidentiality	General Privacy and Confidentiality	General Privacy and Confidentiality
	Optional: <ul style="list-style-type: none"> <li>Research</li> <li>Health System Planning</li> <li>Privacy Impact Assessment</li> <li>'Privacy by Design' Privacy Req'ts for new projects</li> <li>Privacy Brown Bag Lunches on policies, tools, best practices</li> </ul>	Respecting Patient/Client Privacy	Respecting Patient/Client Privacy	HIA Overview	HIA Overview	HIA Overview	HIA Overview	HIA Overview
		Privacy Safeguards	E-Privacy (admin or user)	Respecting Patient/Client Privacy	Respecting Patient/Client Privacy	Respecting Patient/Client Privacy	Respecting Patient/Client Privacy	Respecting Patient/Client Privacy
				Privacy Safeguards	Privacy Safeguards	Privacy Safeguards	Privacy Safeguards	Privacy Safeguards
						E-Privacy (admin or user)	Access & Correction	"Incident Investigation" & Privacy Breach
						Access & Correction	Complex Consent	Access & Correction
								HIA Designated Contact Person Responsibilities
								Complex Consent
								Train the Trainer & Refresh

# Health and Social Services Masking Policy

---

## Policy Statement

A consistent approach to masking ensures that personal health information within electronic health information systems used by the Department of Health and Social Services and the Health and Social Services Authorities is maintained in a manner that complies with consent conditions.

## Scope

This Policy applies to all electronic health information systems used by the Department of Health and Social Services and Health and Social Services Authorities with the technical capability of applying masking methods.

## Definitions

The following terms apply to this Policy:

“Breaking the glass” means a process of temporarily unblocking masked personal health information.

“Consent condition” includes an express instruction and refers to a limit, set by an individual or substitute decision maker, on how the Department/HSSAs may collect, use or disclose personal health information about the individual.

“Electronic health information systems” means those systems designated under the *Health Information Act* with the technical capability of applying masking methods.

“Employee” for the purpose of this Policy means all individuals employed by the Department or HSSA including contracted, salaried or locum health practitioners and individuals whose positions are federally funded.

“Established institutional practice standards” means a practice which guides the Department/HSSA’s behavior, i.e. Accreditation Canada Guidelines, Ministerial Directives, any policies, procedures, guidelines, and standards adopted/established by the Department/HSSAs.

“Established professional practice standards” means a practice that sets out the professional basis for practice and standards of practice, i.e. code of ethics that is recognized, adopted, or established by professional licensing bodies or Canadian professional associations.



"Express instructions" are specific directions provided by an individual or substitute decision maker about how the individual's personal health information may or may not be, collected, used or disclosed that must be clearly documented on the individual's record so that anyone who accesses the record will be aware of them.

"Health and Social Services Authorities" refers to the Northwest Territories Health and Social Services Authority and Boards of Management under the *Hospital Insurance and the Health and Social Services Administration Act*.

"Masking" means a process of obscuring/concealing individual(s)' personal health information in order to prevent, limit, and/or control it from being exposed to individual(s) not authorized to view/access it.

"Personal health information" means information in any form that identifies an individual, or in respect of which it is reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual:

- (a) information about the health and health care history of an individual,
- (b) information respecting health services provided to an individual,
- (c) information about eligibility or registration of an individual for a health service or related product or benefit,
- (d) information about the payment for a health service for an individual,
- (e) information collected in the course of providing a health service to an individual or information that is collected incidentally to the provision of a health service to an individual, including the individual's name and contact information,
- (f) a personal health number, other identifying number, symbol, or other particular assigned to an individual in respect of health services or health information,
- (g) prescribed information about a health service provider that provides a health service to an individual,
- (h) information respecting the donation by an individual of a body part or bodily substance,
- (i) information prescribed as personal health information in the Health Information Regulations.

"Substitute decision maker" means a person, recognized under the *Health Information Act* who is:

- (a) the individual's guardian or parent or person with lawful custody, if the individual is under 19 and is not a mature minor,
- (b) the individual's guardian, trustee, or legal representative,
- (c) a person who holds the individual's power of attorney or the person named in a personal directive,

- (d) anyone authorized in writing by the individual when the individual was mentally competent
- (e) a deceased individual's personal representative, estate executor, or spouse,
- (f) a deceased individual's relative or an adult who had a close personal relationship with the individual,
- (g) a deceased individual's substitute decision-maker identified by the *Human Tissue Donation Act*,
- (h) a prescribed person in prescribed circumstances

and who:

- a. makes decisions on behalf of an individual about their personal health information, **while**
- b. considering the individual's wishes and beliefs, **and**
- c. assessing the benefits against the risks before making a decision.

"Unmasking" means a process used to remove masking permanently.

## Provisions

- 1) The Department/HSSA is responsible for developing masking procedures applicable to their electronic health information systems.
- 2) Masking and unmasking may only be performed by authorized employees identified by the Department/HSSA in accordance with approved masking procedures as amended from time to time by the Department/HSSA.
- 3) Masking and unmasking may only be requested by the individual the information is about, or by the individual's substitute decision maker.
- 4) Masking may not be applied to the following demographic information :
  - Date of birth;
  - Name; and,
  - Personal health care number.
- 5) Masking must not cause harm or result in threat to the individual's safety.
- 6) Masking cannot prohibit or restrict the recording of any information that is required by law or by established institutional or professional practice standards.
- 7) Masking cannot prohibit or restrict the recording of any information that is for the purposes of a program established under the *Pharmacy Act* to monitor prescriptions.

- 8) Masking must be repeatable and reversible so that masked information can be temporarily unblocked, unmasked, and masked again.
- 9) Masking must be documented
  - A record of the individual's consent condition requiring masking must be kept.
  - Any request by an individual to have unmasking performed must be received in writing and recorded.
- 10) Breaking the glass may be performed by any employee or healthcare provider and is permitted:
  - in a medical and/or care emergency where an individual's safety is at risk;
  - when there is a serious risk of harm to the individual, others and/or the public;
  - when a disclosure of information is required by law
- 11) Breaking the glass must be
  - documented along with the reasons and/or circumstances;
  - audited to ensure compliance with the HIA and this policy;
  - reported to authorized employees;
    - i. if the electronic health information system does not automatically re-mask this information, this employee must ensure that making is reapplied as soon as possible
  - reported to the individual whose information was temporarily unblocked, or to the individual's substitute decision maker.

## Authority and References

*Access to Information and Protection of Privacy Act*

*Health Information Act*

Ministerial Directive 2016-02: Privacy Standards, Policies and Standards

Consent Conditions Policy

  
\_\_\_\_\_  
Deputy Minister  
  
  
\_\_\_\_\_  
Date

# MINISTERIAL DIRECTIVE

## Privacy Standards, Policies and Procedures

MD-2017-03

---

### 1. Background

The Department of Health and Social Services (Department) is developing operational privacy standards, policies and procedures to assist custodians of personal health information in complying with the *Health Information Act* and, where applicable, the *Access to Information and Protection of Privacy Act* for personal information.

The policies are being drafted in stages. The following attached Policies have been approved by the Deputy Minister and are effective on the date signed:

- Privacy Breach Policy
- Consent Conditions
- Electronically Stored and Transferred Information Policy
- De-Identification Policy
- Contractor Compliance Policy
- Privacy Impact Assessment Policy
- Masking Policy
- Mandatory Training Policy

The schedule to this Directive is a list of all of the other standards, policies and procedures that will be developed in the near future. Once they are approved and distributed by the Deputy Minister, they are subject to this Directive.

### 2. Purpose

The purpose of this Directive is to ensure that the Department and all Health and Social Services Authorities (HSSAs) have consistent privacy standards, policies and procedures to follow. The standards, policies and procedures and schedule to this Directive may be amended from time to time by the Deputy Minister.

This Directive requires that Department and HSSA staff follow the approved privacy standards, policies and procedures referred to in this Directive.

## MINISTERIAL DIRECTIVE

### Privacy Standards, Policies and Procedures

MD-2017-03

---

#### 3. Definitions

Health and Social Services Authorities refers to the Northwest Territories Health and Social Services Authority and Boards of Management under the *Hospital Insurance and Health and Social Services Administration Act*.

#### 4. Exceptions and Restrictions

None.

#### 5. Amendment

This Directive may be amended in writing by the Minister from time to time.

#### 6. Effective Date

This Directive comes into effect on the date of signing.



Glen Abernethy  
Minister of Health and Social Services

May 8/2017  
Date

# MINISTERIAL DIRECTIVE

## Privacy Standards, Policies and Procedures

MD-2017-03

### SCHEDULE

Pending Privacy Standard, Policy or Procedure *	
1.	Data Excerpt Policy
2.	Auditing Policy
3.	Release of Information Policy, with appendix guidelines for: <ul style="list-style-type: none"><li>- Research vs. Health System Planning</li><li>- Accessing Minor Information</li><li>- Family of Deceased's Right to Information</li><li>- Record of Disclosure</li><li>- Release of Information to Information Privacy Commissioner</li><li>- Disclosure of Information to Officials in Official Capacity</li></ul>
4.	Withdrawing Consent Policy
5.	Recording Device Policy
6.	Electronic Information System Access Management Policy

\*The title of the approved Privacy Standard, Policy or Procedure may vary slightly.



# Health and Social Services Privacy Breach Policy

---

## Policy Statement

A consistent approach in handling both potential and confirmed privacy breaches is necessary across the health and social services system to support the commitment to protect patient and client privacy and minimize the risk of recurrence.

## Scope

This Policy applies to:

- 1) Any potential or confirmed privacy breach of personal information or personal health information of the Department of Health and Social Services (Department) and Health and Social Services Authorities (HSSAs) ; and
- 2) All employees in the Department and HSSAs.

## Definitions

The following terms apply to this Policy:

“Authorized Employee” means an employee who have been authorized by the Department and each HSSA to handle privacy breaches.

“Employee” for the purpose of this Policy means all individuals employed by the Department or HSSA including salaried, contracted or locum health practitioners and individuals whose positions are federally funded.

“Health and Social Services Authorities” (HSSAs) refers to the Northwest Territories Health and Social Services Authority and Boards of Management under the *Hospital Insurance and Health and Social Services Administration Act*.

“Personal information” means information about an identifiable individual, including

- (a) the individual's name, home or business address or home or business telephone number,
- (b) the individual's race, colour, national or ethnic origin or religious or political beliefs or associations,
- (c) the individual's age, sex, sexual orientation, marital status or family status,
- (d) an identifying number, symbol or other particular assigned to the individual,
- (e) the individual's fingerprints, blood type or inheritable characteristics,



- (f) information about the individual's health and health care history, including information about a physical or mental disability,
- (g) information about the individual's educational, financial, criminal or employment history,
- (h) anyone else's opinions about the individual,
- (i) the individual's personal opinions, except where they are about someone else.

"Personal health information" means information in any form that identifies an individual, or in respect of which it is reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual:

- (a) information about the health and health care history of an individual,
- (b) information respecting health services provided to an individual,
- (c) information about eligibility or registration of an individual for a health service or related product or benefit,
- (d) information about the payment for a health service for an individual,
- (e) information collected in the course of providing a health service to an individual or information that is collected incidentally to the provision of a health service to an individual, including the individual's name and contact information,
- (f) a personal health number, other identifying number, symbol, or other particular assigned to an individual in respect of health services or health information,
- (g) prescribed information in the Health Information Regulations about a health service provider that provides a health service to an individual,
- (h) information respecting the donation by an individual of a body part or bodily substance,
- (i) information prescribed as personal health information in the Health Information Regulations.

"Privacy Breach" means an unauthorized use, disclosure, alteration, destruction, disposal, loss or theft of personal information or personal health information.

"Schedule 1" – means the Initial Reporting Schedule, as amended from time to time, attached to this Policy.

"Schedule 2" – means the Investigation Schedule, as amended from time to time, attached to this Policy.

"Schedule 3" – means the Notification Schedule, as amended from time to time, attached to this Policy.

"Schedule 4" – means the Response Schedule, as amended from time to time, attached to this Policy.

"Schedule 5" – means the Final Reporting Schedule, as amended from time to time, attached to this Policy.

## **Provisions**

*Note: The responsibilities assigned to the Authorized Employee in the provisions below may be designated to other individuals as determined by the Department or HSSA if necessary.*

1. The Department and HSSAs must each authorize one or more employees to handle privacy breaches in accordance with this Policy and its Schedules, as amended from time to time.
2. The Department and HSSAs must comply with this Policy and its Schedules, as amended from time to time.
3. All detected potential privacy breaches must be reported to the Authorized Employee (see Schedule 1).
4. HSSAs, including their legal counsel, must report all potential and confirmed privacy breaches to the Department (see Schedule 1, Schedule 3 and Schedule 5).
5. The Authorized Employee must review all reported potential privacy breaches (see Schedule 2).
6. The Department and HSSAs must put in place immediate mitigation measures as part of handling and responding to potential and confirmed privacy breaches (see Schedule 4).
7. The Department or HSSA must carry out a full investigation of all confirmed privacy breaches and where an initial review finds a likelihood of a potential privacy breach (see Schedule 2).
8. Upon confirmation of a privacy breach at the conclusion of a full investigation, the Department or HSSA must notify affected individuals, and other individuals, such as the NWT Information and Privacy Commissioner and law enforcement officials if the circumstances warrant. (See Schedule 3).
9. The Department or HSSAs must prepare a communications plan when the Department or HSSA anticipates the need to provide information about a privacy breach to the media or the general public.
10. The Department and/or HSSAs must determine and ensure the implementation of long-term response measures to address confirmed privacy breaches and to prevent similar privacy breaches from occurring in the future (see Schedule 4).
11. The Department and HSSA must prepare and disseminate final privacy breach reports for confirmed privacy breaches (see Schedule 5).

12. The Authorized Employee must keep records of all potential and confirmed privacy breaches in accordance with approved records schedules.
13. For all potential and confirmed privacy breaches, the Authorized Employee must keep an internal tracking system, which address at a minimum:
  - a. Where and when a breach occurred;
  - b. The type of breach i.e. unauthorized use, disposal or disclosure, theft, loss;
  - c. The media of the breach i.e. email, paper, electronic information system;
  - d. The nature of the breach activity i.e. intentional, accidental, vexatious; and
  - e. The number of individuals affected.

## Exceptions

1. If a potential or confirmed privacy breach involves information governed by the *Child and Family Services (CFS) Act*, this Policy must be followed but any changes necessary to comply with the CFS Act may be made.
2. If a potential or confirmed privacy breach relates to a current proceeding to which the Department or HSSA is a party, Legal Counsel must be consulted with prior to applying this Policy. Follow legal advice instead of the provisions in this Policy, to the extent of the conflict.

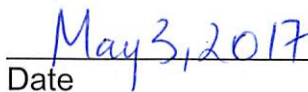
## Authority and References

*Access to Information and Protection of Privacy Act*

*Health Information Act*

Ministerial Directive 2016-02: Privacy Standards, Policies and Standards  
Schedules 1-5 to the Privacy Breach Policy, as amended from time to time.

  
\_\_\_\_\_  
Deputy Minister

  
\_\_\_\_\_  
Date

## **SCHEDULE 1: INITIAL REPORTING**

Department and HSSA employees must report all detected potential privacy breaches as soon as reasonably possible to an Authorized Employee.

An employee reporting a detected potential privacy breach must:

- Report the detected potential privacy breach to an Authorized Employee, and such report may include:
  - A description of the situation;
  - A reason or explanation why the situation is of concern;
  - Date(s) and time(s) of the event;
  - Person(s) involved in / causing the concerned behaviour; and
  - Any action(s) taken to date to stop the behaviour;
- Provide any relevant evidence, i.e. notes or related documents;
- Maintain privacy and confidentiality during and after reporting; and
- Follow any directions received by the Authorized Employee in response to their reporting.

If an employee receives a complaint from a member of the public indicating a potential privacy breach, the employee must report this to an Authorized Employee as soon as reasonably possible.

The Department / HSSA must ensure no harm or action is taken against an employee who reports a detected potential privacy breach if done so in good faith.

An HSSA Authorized Employee who receives a report of a potential privacy breach must report the potential privacy breach to the Department for tracking purposes as soon as reasonably possible. All efforts should be made not to share identifiable information as part of this report.

Where the Department / HSSA receives a report of a potential privacy breach, it must comply with Schedule 2.

## **SCHEDULE 2: INVESTIGATION**

The Authorized Employee must carry out an initial review of every detected potential privacy breach. The Department / HSSA must carry out a full investigation whenever an initial review reveals a potential or confirmed privacy breach.

The Department / HSSA must document the initial review and full investigation, including:

- Details around the process and progress of the initial review and full investigation (reports, status updates)
- Evidence collected, secured, and examined (including observation and details of the scene, where/how privacy breach occurred)
- Recorded interviews conducted and interview notes
- Subject matter expert(s) testimony(s)

The Department / HSSA must carry out initial reviews and investigations in a manner that respects procedural fairness to ensure:

- Quality evidence is collected
- Evidence is collected appropriately
- Evidence establishes facts on which any findings of potential privacy breach is based.

The Department / HSSA must ensure employees cooperate during an initial review and full investigation.

Employees must provide any requested details and items (i.e. information / documents / devices) for evidence gathering purposes, subject to legislation, and must not interfere with an initial review and full investigation.

The Department / HSSA must carry out requirements set out in this Schedule concurrently with immediate mitigation measures set out in Schedule 4.

### **1. Initial Review**

The Authorized Employee must complete an initial review of every detected potential privacy breach whether it was reported by an employee or brought to the attention of the Department / HSSA through a complaint by a member of the public.

An initial review consists of a preliminary gathering of evidence related to the potential privacy breach.

Based on the findings of the initial review, the Authorized Employee will determine the status of the potential privacy breach:

- No privacy breach;
- Potential privacy breach; or
- Confirmed privacy breach.

Where the initial review reveals that the evidence shows no indication of a privacy breach:

- The Authorized Employee leading the initial review must ensure details describing the nature of the incident and details of the initial review are documented, (who, what, when, where, how) should this information be required in future for reference.
- Where the notice of a potential privacy breach has been received / driven by a complaint, the Authorized Employee must inform the individual(s) that the initial review determined no privacy breach occurred.

Where the initial review finds a likelihood of a potential privacy breach, the Department / HSSA must carry out a full investigation as set out below.

Where the initial review confirms the occurrence of a privacy breach, the Authorized Employee may proceed to notification as set out in Schedule 3.

## **2. Full Investigation**

The Deputy Minister of the Department / Chief Executive Officer of the HSSA may:

- Authorize an investigator(s) (internal or external);
- Assign an Authorized Employee to carry out a full investigation;
- Authorize and assign additional person(s) to assist during a full investigation e.g. technical support;
- Consider impacts on operations as a result of the full investigation; and
- Make decisions based upon the investigator's findings and recommendations.

The Deputy Minister of the Department / Chief Executive Officer of the HSSA maintains discretion in determining whether:

- to have an external / internal investigator; and
- an authorized investigator may carry out the investigation where a potential conflict of interest has been identified (see Investigator Selection section).

The Department / HSSA is required to determine based on factors, set out in this Schedule, if an Authorized Employee, internal or external investigator will be used.

The Department/ HSSA must consider the following factors in determining whether an external investigator would be more appropriate to lead the investigation:

- Where the use of an Authorized Employee or internal investigator would lead to a real or perceived conflict of interest, or lack of independent analysis, objectivity and/or public transparency;
- Where appropriate expertise or skill set is not available in the organization; and
- Where a real or perceived magnitude of risk of harm associated with the potential privacy breach necessitates an objective, arms-length investigator.

If using an external investigator, they must have a contract.

If using an internal investigator, they must be formally assigned to the role, if not already in their job description/regular job duties.

The Department/ HSSA must prepare a statement of work or terms of reference for an external investigator in accordance with this Schedule.

The statement of work guides the investigation and may include but not be limited to:

- What discrepancy/suspected violation/situation/inappropriate action is the focus of the investigation;
- Types of evidence to be collected;
- Mean by which evidence of various modes will be protected/secured (physically, electronically, etc.);
- Identify content and types of questions to be asked during interviews (ensuring appropriately structured questions);
- Timeline for completion of the investigation and deadline for reporting; and
- Prevention steps for scenario if investigation is discontinued.

The scope of the investigation must be determined and may be based on:

- Preliminary judgment(s) made about the details of the notice received and initial review finding(s);
- The seriousness of the privacy breach (i.e. magnitude of the privacy breach, level of harm caused by the privacy breach); and
- Discovery of additional evidence, as the investigation progresses.

The role of the investigator (Authorized Employee, internal or external investigator) is to assist, lead or conduct an investigation and may include, but not be limited to:

- Reviewing the initial review findings;

- Gathering evidence, conducting interviews, gathering relevant documents (i.e. employee interviews, handwritten notes, audio/visual recordings, digital devices etc.);
- Identification of the personal and/or personal health information in question;
- Calling on technical support within the Department / HSSAs;
- Consulting with the appropriate resources, including Legal, Human Resources, HIA Designated Contact Person prior to interviewing staff;
- Determining the risk of harm to affected individuals and the risk of harm to the Department / HSSA, such as loss of public trust, identity theft, financial exposure, loss of assets, and legal liability;
- Making findings based on evidence, as to if a privacy breach occurred (nature of breach, involved parties, reason/cause of breach, breach impact(s), resulted harm, number of individuals affected etc.); and
- Making recommendation(s) related to response measures, remediation that should occur.

The investigation can expand, subject to the severity of the privacy breach and whether it is a systemic breach.

Where the full investigation confirms the occurrence of a privacy breach, the Department / HSSA must comply with Schedule 3, Schedule 4, and Schedule 5.

### **3. Investigator Selection**

When authorizing or hiring an investigator (internal or external) the Department / HSSA must review and ensure the candidate has suitable / adequate abilities and skills for the role.

Key abilities and skills an investigator should have may include but are not limited to:

- Knowledge of the health and social services system and governance structure in the NWT;
- Knowledge of privacy legislation and health specific privacy legislation (HIA, ATIPP);
- Sound skills in gathering evidence and procedural fairness;
- Ability to be objective, unbiased and independent;
- Capacity to assess, interpret and weigh on conflicting evidence for the purpose of making findings of fact; and
- Ability to maintain privacy and confidentiality while carrying out investigation.



Where an external investigator is selected, they are required to comply with the statement of work or terms of reference received and this policy.

Potential investigators must identify any possible conflict of interest and communicate this to the Deputy Minister of the Department / Chief Executive Officer of the HSSA or their delegate.

### **SCHEDULE 3: NOTIFICATION**

Where the privacy breach has been **confirmed** upon the completion of a full investigation as set out in Schedule 2, the Department / HSSA must carry out privacy breach notifications in accordance with this Schedule.

In addition, the Department / HSSA may decide to notify the NWT Information and Privacy Commissioner and Risk Management and Insurance of potential privacy breaches prior to the completion of a full investigation.

The Department / HSSA responsible for the confirmed privacy breach must notify via formal communication (letter):

- The affected individual(s);
- The NWT Information and Privacy Commissioner, if:
  - The confirmed privacy breach involves unauthorized disclosure of personal information or personal health information;
  - The confirmed privacy breach involves theft of personal information or personal health information; or
  - There is a reasonable risk of harm to an affected individual as a result of a confirmed privacy breach involving the unauthorized use, alteration, destruction, disposal, or loss of personal information or personal health information;
- Law Enforcement Officials, if personal information or personal health information is:
  - Lost or stolen; or
  - Disclosed, altered, destroyed or otherwise disposed of, through fraud or identity theft;
- The Office of the Chief Information Officer, if the privacy breach involves electronic systems, a GNWT (Government of the NWT) server, GNWT hardware, or email in a systemic or large scale manner;
- Risk Management and Insurance;
- The GNWT Comptroller General, if:
  - the privacy breach involves the theft, loss or destruction (see Financial Administration Manual 215 – Loss of Assets) of information, which is considered a GNWT asset;

In the case of an HSSA responsible for a confirmed privacy breach, the HSSA must notify the Department.

The Department / HSSA must ensure the Union is notified whenever temporary or permanent disciplinary measures are taken in response to a privacy breach. Notification should come from the appropriate Human Resources representative.

The Department / HSSA should also consider whether any other authorities or organizations should be informed of the breach, for example:

- Technology suppliers if the breach was due to a technical failure and a recall or technical fix is required;
- Other internal or external parties not already notified that may have been impacted by the breach such as third party contractors or internal program and services area.

The Department / HSSA may use discretion to determine if it is appropriate and reasonable to notify a professional or other regulatory body, if a privacy breach full investigation has identified suspected professional misconduct.

Notification letters may be prepared by an Authorized Employee.

If law enforcement requests a delay in notification because the notification could prejudice an active law enforcement matter, the Department / HSSA, should delay notification upon written request from the law enforcement official requesting the delay and specifying the time period of the delay. If an oral request is made, the Department/ HSSA should delay notification and make a record of the request and the law enforcement official making the statement.

If notification relates to information under the *Mental Health Act*, special consideration must be given to the *Mental Health Act* s.98, once the Act comes into force, and the application of this Schedule must be modified to ensure compliance with *Mental Health Act*.

If notification to affected individuals is hindered by a lack of, or concerns around, contact information, consideration should be given to alternative ways of gathering accurate and reliable contact information without jeopardizing the individual's privacy. All reasonable efforts must be made to contact affected individuals.

If a privacy breach is significant enough to require a communications plan, the plan must address communications with others (i.e. employees, MLAs) that will be necessary as a result of notifications required under this Schedule.

**The following is a breakdown of what information must be included and what should not be included in notifications to specified parties.**

**NOTE:** Prior to sending notification letters the DM / CEO must be briefed in a manner that respects the privacy of affected individuals.

### **1. Privacy Breach Notification to an Affected Individual(s)**

The Department / HSSA responsible for a confirmed privacy breach must notify the affected individual(s) via formal communication (letter) unless this type of notification is not appropriate or possible. The notification should include:

- where and when the breach occurred;

- the type of breach i.e. unauthorized use, disposal or disclosure, theft, loss;
- the media/form of information breached i.e. paper, electronic, verbal;
- the nature/subject of the information breached i.e. medical, mental health, child and family services;
- the type of documents/records of the information breached , i.e. patient chart, laboratory results, case notes;
- Risk(s) to the individual caused by the breach, if applicable and known;
- an overview of any immediate actions taken or changes made in response to/to mitigate/manage the breach;
- a commitment to take future steps to prevent further privacy breaches;
- steps the individual can take to further mitigate the risk of harm (e.g. how to contact credit reporting agencies to set up a credit watch if applicable);
- contact information of an employee with the Department / HSSA who can answer questions or provide further information; and
- Information and Privacy Commissioner contact information and the fact the individuals have a right to ask for a review by the Information and Privacy Commissioner.

**Information that should not be included in a notification:**

- other individuals' personal information including their name;
- employee's personal information including their name;
- information that could change as a result or compromise ongoing investigations; and
- details of the investigation or response.

**2. Notification Template for the NWT Information and Privacy Commissioner**

The Department / HSSA responsible for a confirmed privacy breach must notify the NWT Information and Privacy Commissioner (IPC) in accordance with mandatory notification set out in this Schedule. A formal notification to the IPC is only required if the incident is confirmed as a privacy breach. The notification should include:

- where and when the breach occurred;
- the type of breach i.e. unauthorized use, disposal or disclosure, theft, loss;
- the media/form of information breached i.e. paper, electronic, verbal;
- the nature/subject of the information breached i.e. medical, mental health, child and family services;

- the type of documents/records of the information breached , i.e. patient chart, laboratory results, case notes;
- the number of individuals known or suspected who were affected and if or when they were or will be notified; and
- an overview of any immediate actions taken or changes made in response to/to mitigate/manage the breach.

Information that should not be included in a notification:

- client's personal health information including their name;
- employee's personal information including their name;
- information that could change as a result or compromise ongoing investigations; and
- details of the investigation or response.

If the IPC initiates a review under ATIPP and requests more information or specific records, or at any time requests information or specific records under HIA, whether there is a review or not, the Department / HSSA must provide all the requested material.

If the request is made as a part of a review under HIA, the Department / HSSA must provide the material within 14 days.

### **3. Privacy Breach Notification to the Department (from a HSSA)**

An HSSA responsible for a confirmed privacy breach must notify the Department. The notification should include:

- where and when the breach occurred;
- the type of breach i.e. unauthorized use, disposal or disclosure, theft, loss;
- the media/form of information breached i.e. paper, electronic, verbal;
- the nature/subject of the information breached i.e. medical, mental health, child and family services;
- the type of documents/records of the information breached , i.e. patient chart, laboratory results, case notes;
- the number of individuals known or suspected who were affected and if or when they were or will be notified;
- an overview of any immediate actions taken or changes made in response to/to mitigate/manage the breach;
- status of investigation or response;
- whether the IPC has been notified;

- whether breach is suspected to be intentional, accidental, vexatious or not; and
- number of staff implicated.

**Information that should not be included in a notification:**

- client's personal health information including their name;
- employee's personal information including their name; and
- other's personal information.

**4. Privacy Breach Notification to Law Enforcement Officials**

The Department / HSSA must notify law enforcement if the confirmed breach involves criminal activity in accordance with this Schedule. The Department / HSSA should provide notice as soon as reasonably possible to halt any potential criminal activity or to seek justice. The notification should include:

- where and when the breach occurred;
- nature of potential theft, criminal activity etc.;
- name of individual(s) suspected in the incident; and
- any relevant further information requested by law enforcement that would aid them in their investigation.

**5. Privacy Breach Notification to the Office of the Chief Information Officer (OCIO)**

The Department / HSSA must notify the OCIO if the confirmed breach involves electronic systems, a Government of the NWT (GNWT) server, GNWT hardware, or email in a systemic or large scale manner. The notification should include:

- where and when the breach occurred;
- the type of breach i.e. unauthorized use, disposal or disclosure, theft, loss;
- the specific electronic system affected;
- the nature/subject of the information breached i.e. medical, mental health, child and family services;
- the type of documents/records of the information breached i.e. patient chart, laboratory results, case notes; and
- an overview of any immediate actions taken or changes made in response to/to mitigate/manage the breach.

**Information that should not be included in notification:**

- client's personal information including their name;

- employee's personal information including their name;
- details of investigation; and
- other's personal information.

## **6. Privacy Breach Notification to Risk Management and Insurance**

The Department / HSSA must notify Risk Management and Insurance of a confirmed breach.

- The notification should include:
  - where and when the breach occurred;
  - the type of breach i.e. unauthorized use, disposal or disclosure, theft, loss;
  - the media/form of information breached i.e. paper, electronic, verbal;
  - the nature/subject of the information breached i.e. medical, mental health, child and family services;
  - the number of individuals known or suspected who were affected and if or when they were or will be notified;
  - any potential/possible risk of harm or liability to organization; and
  - an overview of any immediate actions taken or changes made in response to/to mitigate/manage the breach.

### **Information that should not be included in notification:**

- client's personal information including their name;
- employee's personal information including their name;
- details of investigation; and
- other's personal information.

## **7. Privacy Breach Notification to the Comptroller General**

The Department / HSSA must notify the Comptroller General of a confirmed breach, if

- The breach involves the theft, loss or destruction (see Financial Administration Manual 215 – Loss of Assets) of information, which is considered a GNWT asset. The notification should include:
  - where and when the breach occurred;
  - the type of breach i.e. unauthorized use, disposal or disclosure, theft, loss;

- the media/form of information breached i.e. paper, electronic, verbal;
- the nature/subject of the information breached i.e. medical, mental health, child and family services;
- the number of individuals known or suspected who were affected and if or when they were or will be notified;
- any potential/possible risk of harm or liability to organization; and
- an overview of any immediate actions taken or changes made in response to/to mitigate/manage the breach.

**Information that should not be included in notification:**

- client's personal information including their name;
- employee's personal information including their name;
- details of investigation; and
- other's personal information.

## **8. Privacy Breach Notification to the Union**

The Department / HSSA must ensure the Union is notified whenever temporary or permanent disciplinary measures are taken in response to a confirmed privacy breach. Notification should come from the appropriate Human Resources representative. The notification should include:

- employee's personal information including their name;
- the nature of the employee's disciplinary issues in relation to a privacy breach that required temporary or permanent disciplinary measures to be taken;
- whether the employee has been involved in similar breach or disciplinary issue in the past;
- any documentation of previous relevant training received by the employee;
- any relevant Department / HSSA policies, procedures, notices to staff; and
- any relevant further information upon the advice of the Human Resources representative.

**Information that should not be included in notification:**

- client's personal information and personal health information including their name;
- details of investigation; and
- the specific documents / records of the information breaches, i.e. patient chart, laboratory result, case notes.



## **9. Privacy Breach Notification to Professional and Regulatory Bodies**

The Department / HSSA may use their discretion, after consultation with the appropriate Human Resources representative, in deciding whether to notify a professional or other regulatory body if professional misconduct is suspected in relation to a confirmed privacy breach. The notification should include:

- where and when the breach occurred;
- the type of breach i.e. unauthorized use, disposal or disclosure, theft, loss;
- the media/form of information breached i.e. paper, electronic, verbal;
- the nature/subject of the information breached i.e. medical, mental health, child and family services;
- the specific documents/records of the information breached , i.e. patient chart, laboratory results, case notes;
- employee's personal information including their name;
- suspected professional misconduct;
- any documentation of previous relevant training received by the employee; and
- any relevant further information requested by an authorized representative of the professional or regulatory body that would aid them in their investigation.

## **SCHEDULE 4: RESPONSE**

While mitigating and responding to potential and confirmed privacy breaches, the Department / HSSA must take appropriate safeguard measures to ensure the maintenance of privacy and confidentiality, including:

- treating evidence as confidential;
- avoiding unnecessary further disclosure of information;
- protecting the identity of employees and individuals involved in the situation; and
- appropriately managing communications, including messaging to the public, balancing public accountability and transparency with responsibility to protect clients, employees, the organization and the health and social services system from undue harm.

An assigned Department / HSSA authorized employee responsible for handling privacy breaches must be available on a continual basis to respond to any incoming inquiries relating to a potential or confirmed privacy breach.

### **1. Immediate Mitigation**

The Department / HSSA must take immediate steps to mitigate and manage a privacy breach situation. Measures taken must stop or limit the spread of a potential or confirmed privacy breach and start to respond to a breach.

Immediate mitigation measures that may be taken include, but are not limited to:

- Recovering records;
- Shutting down an information system;
- Inactivating accounts or changing access privileges;
- Suspending contract services;
- Restricting planned data extracts;
- Destroying unauthorized copies of information, documenting the destruction;
- Developing and implementing interim corrective measures until formal new procedures are approved and implemented;
- Providing interim on-the-job coverage or support; and
- Temporary or permanent disciplinary measures, including changes to clinical privileges.

The Department / HSSA must ensure mitigation measures respond to the root cause(s) of a privacy breach.

The Department / HSSA must ensure mitigation measures are reasonable and proportional to the risk of harm associated with the privacy breach.

The Department / HSSA may consult and discuss mitigation measures with other bodies as necessary or appropriate.

Where potential employee disciplinary issues become apparent during an initial review or full investigation, the Department / HSSA must immediately report these issues to the appropriate Human Resource representative and work with this representative to determine if temporary or permanent disciplinary measures may be necessary as part of immediate mitigation measures taken. In the case that temporary or permanent disciplinary measures are to be taken in relation to a privacy breach, the Department / HSSA must work with the appropriate Human Resources representative to ensure the union is properly notified.

Where the Department / HSSA was in touch with a Human Resources representative during an initial review or full investigation in respect of immediate mitigation measures that took the form of disciplinary measures, the organization must follow up with the Human Resources representative upon completion of the initial review and upon completion of the full investigation to review the appropriateness of these disciplinary measures.

## **2. Long-Term Response**

The Department / HSSA must determine, based on full investigation findings and recommendations, what long-term response measures are to be taken to address the privacy breach and to prevent a similar privacy breach from occurring in the future.

Long-term response measures that may be taken include, but are not limited to:

- Development or delivery of additional training;
- Development or implementation of additional auditing;
- Revised policies, directives, procedures, or standards;
- Revised administrative, technical, or physical privacy and security safeguards;
- Revised job duties or job descriptions;
- Temporary or permanent disciplinary measures;
- Amendments to contracts and information management agreements; and
- Contract termination.

The Department / HSSA must ensure long-term response measures respond to the root cause(s) of a privacy breach.

The Department / HSSA must ensure long-term response measures are reasonable and proportional to the risk of harm associated with the privacy breach and the risk of recurrence.

The Department / HSSA may consult and discuss proposed long-term response measures with other bodies as necessary or appropriate.

Where a full investigation confirms employee disciplinary issues, the Department / HSSA must report these issues to the appropriate Human Resource representative and work with this representative to determine if temporary or permanent disciplinary measures may be necessary as part of long-term response measures taken. In the case that temporary or permanent disciplinary measures are to be taken in relation to a privacy breach, the Department/ HSSA must work with the appropriate Human Resources representative to ensure the union is properly notified.

The Department / HSSA must track the implementation of long-term response measures until such time as they are fully put in place. The Department / HSSA may continue to monitor and evaluate the long-term response measures.

## **SCHEDULE 5: FINAL REPORTING**

The Department / HSSA must complete a final privacy breach report for every confirmed privacy breach.

Mandatory privacy breach reports may be completed by an authorized employee responsible for handling privacy breaches or an investigator.

Final privacy breach reports are subject to access request provisions under ATIPP and HIA. If access requests are received by individuals whose personal information was breached or others, the Department / HSSA responsible for the privacy breach must process the request in accordance with ATIPP and HIA as applicable, keeping in mind legislated exceptions to the right of access.

Final privacy breach reports should document steps taken in accordance with Schedule 1, Schedule 2, Schedule 3 and Schedule 4.

The following is a breakdown of identified parties who must be provided with a final privacy breach report and what information must be included.

### **1. Privacy Breach Final Reporting to the Deputy Minister of the Department or the Chief Executive Officer of an HSSA**

The outcomes of privacy breach investigation must be reported to the DM of the Department/ CEO of the HSSA responsible for the privacy breach. The final report should include:

- Background of what happened and what led to initiate the investigation;
- Findings and presenting the evidence collected, where and what found;
- Analysis, explaining the order of event(s) leading to the privacy breach;
- Recommendation(s) based on findings;
- Immediate mitigation measures taken;
- Long-term response measures to be taken;
- Notifications sent;
- Client's personal health information including their name;
- Employee's personal information including their name; and
- Whether or not any complaints have been made.
- Other's personal information.

Final reporting must be prepared in compliance with this Policy and privacy principles.

## **2. Privacy Breach Final Reporting to the Department (from an HSSA)**

The HSSA must provide a final privacy breach report to the Department. The final report should include:

- Background of what happened and what led to initiate the investigation;
- Findings and presenting the evidence collected, where and what found;
- Analysis, explaining the order of event(s) leading to the privacy breach;
- Recommendation(s) based on findings;
- Immediate mitigation measures taken;
- Long-term response measures to be taken; and
- Notifications sent.

Final reporting must be prepared in compliance with privacy principles. Information that should not be included in the final report includes:

- Client's personal health information including their name;
- Employee's personal information including their name; and
- Other's personal information.

## **3. Privacy Breach Final Reporting to the NWT Information and Privacy Commissioner**

The Department / HSSA responsible for the privacy breach must provide a final report on the privacy breach to the NWT Information and Privacy Commissioner (IPC), where the IPC was previously notified of the privacy breach in accordance with Schedule 3. The final report to the IPC should include:

- Background of what happened and what led to initiate the investigation;
- Findings and presenting the evidence collected, where and what found;
- Analysis, explaining the order of event(s) leading to the privacy breach;
- Recommendation(s) based on findings;
- Immediate mitigation measures taken;
- Long-term response measures to be taken; and
- Notifications sent.

Final reporting must be prepared in compliance with privacy principles. Information that should not be included in the final report includes:

- Client's personal health information including their name;
- Employee's personal information including their name; and
- Whether or not any complaints have been made.

- Other's personal information.

If the IPC initiates a review under ATIPP and requests more information or specific records, or at any time requests information or specific records under HIA, whether there is a review or not, the Department / HSSA must provide all the requested material.

If the request is made as a part of a review under HIA, the Department / HSSA must provide the material within 14 days.

#### **4. Privacy Breach Final Reporting to the Minister of Health and Social Services (Minister)**

For systemic privacy breach, privacy breach of significant magnitude or impact on the health and social services system or the Department/ HSSA, the Department / HSSA responsible for the privacy breach must provide a final privacy breach report to the Minister of Health and Social Services.

The final report to the Minister should include:

- Background of what happened and what led to initiate the investigation;
- Findings;
- Analysis, explaining the order of event(s) leading to the privacy breach;
- Recommendation(s) based on findings;
- Immediate mitigation measures taken;
- Long-term response measures to be taken; and
- Notifications sent.

Final reporting must be prepared in compliance with privacy principles. Information that should not be included in the final report includes:

- Client's personal health information including their name;
- Employee's personal information including their name;
- Details of investigation, interviews, evidence collected; and
- Other's personal information.

For greater clarity one report may be prepared to serve purposes of #1 - #4 and redacted accordingly.

The following is a breakdown of identified parties who **may** be included in final reporting and what information must be included.

## **5. Privacy Breach Final Reporting to the Office of the Chief Information Officer (OCIO)**

The Department / HSSA responsible for the privacy breach may include the OCIO in final reporting, if:

- The OCIO received privacy breach notification; or
- The privacy breach findings and recommendation(s) involve/impact electronic systems, a GNWT (Government of the NWT) server, GNWT hardware, or email in a systemic or large scale manner.

The final report to OCIO should include:

- Redacted Overview/Summary of the privacy breach (i.e. executive summary);
- Recommendation(s);
- Immediate mitigation measure taken; and
- Long-term response measures to be taken.

Final reporting must be prepared in compliance with privacy principles. Information that should not be included in the final report includes:

- Client's personal health information including their name;
- Employee's personal information including their name;
- Details of investigation; and
- Other's personal information.

## **6. Privacy Breach Final Reporting to Risk Management**

The Department / HSSA responsible for the privacy breach must include Risk Management in final reporting:

The final report to Risk Management should include:

- Redacted Overview/Summary of the privacy breach (i.e. executive summary);
- Recommendation(s);
- Immediate mitigation measure taken; and
- Long-term response measures to be taken.

Final reporting must be prepared in compliance with privacy principles. Information that should not be included in the final report includes:



- Client's personal health information including their name, unless a law suit was filed (Risk Management requires the names of the aggrieved parties in the event of a law suit);
- Employee's personal information including their name;
- Details of investigation; and
- Other's personal information.

### **7. Privacy Breach Final Reporting to the Comptroller General**

The Department / HSSA responsible for the privacy breach may include the Comptroller General in final reporting, if:

- Comptroller General received privacy breach notification; or
- The privacy breach findings and recommendation(s) involves the theft, loss or destruction of information which is considered a GNWT asset (see Financial Administration Manual 215 – Loss of Assets).

The final report to Comptroller General should include:

- Redacted Overview/Summary of the privacy breach (i.e. executive summary);
- Recommendation(s);
- Immediate mitigation measure taken; and
- Long-term response measures to be taken.

Final reporting must be prepared in compliance with privacy principles. Information that should not be included in the final report includes:

- Client's personal health information including their name;
- Employee's personal information including their name;
- Details of investigation; and
- Other's personal information.

### **8. Privacy Breach Final Reporting to the Professional Bodies**

The Department / HSSA responsible for the privacy breach may provide Professional Bodies with a final report on the privacy breach upon request, if in relation to a complaint, inquiry, investigation or review under professional licensing legislation and the request is made in accordance with that legislation.

### **9. Privacy Breach Final Reporting to media/public**

The Department / HSSA responsible for the privacy breach may include media/public in final reporting. The final reporting to media/public may occur if:

- Information about the privacy breach has been leaked to the press (i.e. through social media);
- Media/public received initial statement(s) or notification about the privacy breach;
- There is pressure from media/public to disclose information about the privacy breach; or
- There is a need to respond to any negative press.

Final reporting to media/public must occur in accordance with an approved communications plan.

The information to be shared with media/public must be prepared in compliance with privacy principles. Information that must not be shared includes:

- Information that could identify a person including personal information and personal health information about affected individuals and employees, for example, a client's name or an employee's name;
- Details of the investigation, interviews, evidence collected; and
- Sensitive or confidential organizational information, including any information that may put the security of electronic information systems or other assets at risk.

# Health and Social Services Privacy Impact Assessment Policy

---

## Policy Statement

A consistent approach must be used across the health and social services system when determining a need for, and completing Privacy Impact Assessments to ensure that potential privacy risks are correctly identified and managed.

## Scope

This Policy applies to:

- 1) The Department of Health and Social Services (Department) and the Health and Social Services Authorities (HSSAs)
- 2) All employees of the Department and HSSAs
- 3) Any new or proposed change to a health and/or social services project

## Definitions

The following terms apply to this Policy:

“Employees” for the purpose of this Policy means all individuals employed by the Department or HSSA including salaried, contracted or locum health practitioners and individuals whose positions are federally funded.

“Health and Social Services Authorities” refers to the Northwest Territories Health and Social Services Authority and Boards of Management under the *Hospital Insurance and the Health and Social Services Administration Act*.

“Personal information” means information about an identifiable individual, including

- (a) the individual's name, home or business address or home or business telephone number,
- (b) the individual's race, colour, national or ethnic origin or religious or political beliefs or associations,
- (c) the individual's age, sex, sexual orientation, marital status or family status,
- (d) an identifying number, symbol or other particular assigned to the individual,
- (e) the individual's fingerprints, blood type or inheritable characteristics,

- (f) information about the individual's health and health care history, including information about a physical or mental disability,
- (g) information about the individual's educational, financial, criminal or employment history,
- (h) anyone else's opinions about the individual,
- (i) the individual's personal opinions, except where they are about someone else.

"Personal health information" means information in any form that identifies an individual, or in respect of which it is reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual:

- (a) information about the health and health care history of an individual,
- (b) information respecting health services provided to an individual,
- (c) information about eligibility or registration of an individual for a health service or related product or benefit,
- (d) information about the payment for a health service for an individual,
- (e) information collected in the course of providing a health service to an individual or information that is collected incidentally to the provision of a health service to an individual, including the individual's name and contact information,
- (f) a personal health number, other identifying number, symbol, or other particular assigned to an individual in respect of health services or health information,
- (g) prescribed information about a health service provider that provides a health service to an individual,
- (h) information respecting the donation by an individual of a body part or bodily substance,
- (i) information prescribed as personal health information in the Health Information Regulations.

"Privacy impact assessment" means an assessment describing how the privacy of individuals whose personal health information would be collected, used, or disclosed, would be affected by a proposed new or a proposed change to an information system, communication technology, or health and social services project.

"Project" means a health or social services program, initiative, information system, or communication technology.

## Provisions

- 1) It is **mandatory** to complete a Privacy Impact Assessment when a new information system or communications technology is being considered that collects, uses or discloses personal information or personal health information, or when changes are made to existing information systems or communication technologies.
- 2) For all other large scale or significant projects, the approved Privacy Impact Assessment Overview and Decision Tree (Appendix 1), as amended from time to time, must be considered to determine whether a Privacy Impact Assessment is necessary.
- 3) The approved Privacy Impact Assessment Template (Appendix 2), as amended from time to time, must be used when completing the Assessment.
- 4) It is **mandatory** to provide a copy of a Privacy Impact Assessment to the Information and Privacy Commissioner if the program, initiative, information system, or communication technology involves personal health information.

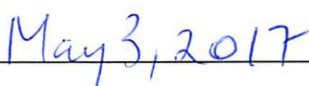
## Authority and References

*Access to Information and Protection of Privacy Act*

*Health Information Act*

Ministerial Directive 2016-02: Privacy Standards, Policies and Standards

  
\_\_\_\_\_  
Deputy Minister

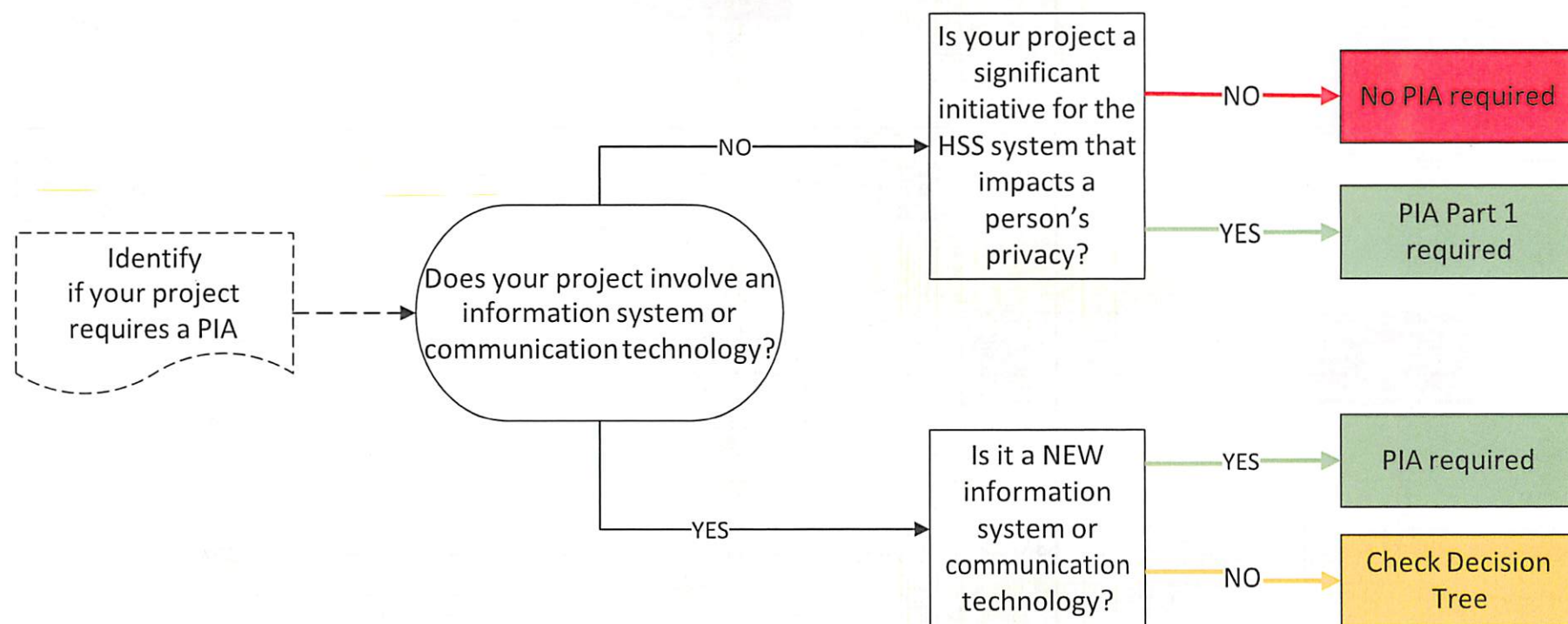
  
\_\_\_\_\_  
Date

Use this OVERVIEW and DECISION TREE (see next page) for guidance around when a PIA **is needed** and when it **is not**.

### Privacy Impact Assessment (PIA) **OVERVIEW** for new or proposed changes to Territorial Health and Social Services (HSS) Projects

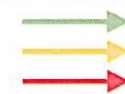
A PIA:

- Identifies privacy risks associated with a new or proposed change to a project and appropriate risk mitigation steps to be taken.
- Should be considered at the planning stage of any project involving an information system, communications technology, or significant initiative of the HSS system.

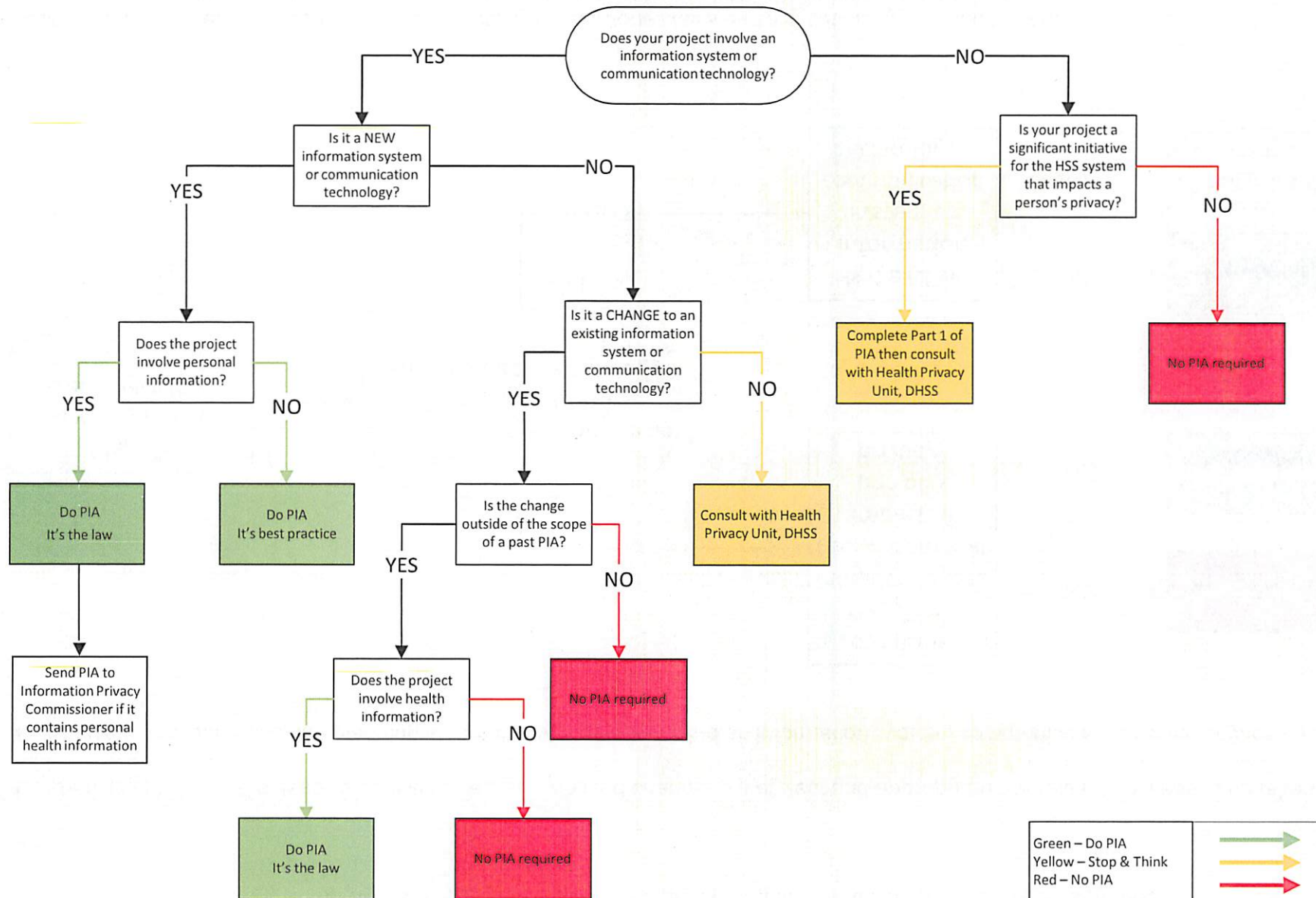


Conducting a PIA ensures compliance with Northwest Territories laws and regulations governing privacy and demonstrates Territorial HSS system's commitment to protect the privacy of residents/clients.

Green – Do PIA  
Yellow – Stop & Think  
Red – No PIA



# Privacy Impact Assessment (PIA) **DECISION TREE** for Territorial Health and Social Services (HSS) Projects





**PRIVACY IMPACT ASSESSMENT**

Submit PIA to:	Health Privacy Unit Policy, Legislation and Communications Department of Health and Social Services Government of the Northwest Territories <a href="mailto:HIA@gov.nt.ca">HIA@gov.nt.ca</a> / 867-767-9052 <b>OR</b> Your Health and Social Services Authority designated representative: Name: Title: Organization: Phone: Email:
Date sent	(DD/MM/YYYY)
Project Name	
Project Manager Contact Information	Name: Title: Division: Organization: Phone: Email:

**DEFINITIONS:**

*"Collect"* means in relation to information to acquire, obtain or receive.

*"Use"* means in relation to information to handle, deal with, apply or transform.

*"Disclose"* means in relation to information to release or make available in any manner.

*"Personal information"* means information about an identifiable individual (see section 2 of the Northwest Territories [Access to Information and Protection of Privacy Act](#)).

*"Personal health information"* means information in any form related to health that identifies an individual, including but not limited to: health care history, health services provided, eligibility or registration for a health service or benefit, health care number (see section 1 of the Northwest Territories [Health Information Act](#)).

*"Privacy impact assessment"* in respect of an information system, communication technology, or health and social services (HSS) initiative means an assessment describing how the privacy of individuals whose information would be collected, used, or disclosed would be affected by the system, technology, or initiative.

*"Project"* is a unified term to include a program, initiative, information system, or communication technology.



## **PURPOSE:**

A Privacy Impact Assessment (PIA) is a process designed to determine how the privacy of individuals would be affected by a new or a proposed change to an information system or communication technology. A PIA may also be done when considering new administrative practices, HSS initiatives, or new programs and services.

Under the Northwest Territories *Health Information Act* (HIA), the territorial HSS system composed of the Department of Health and Social Services (DHSS) and Health and Social Services Authorities (HSSAs) is required to complete PIA(s) when considering a new information system or communication technology, or a change to an existing one.

Current privacy best practices dictate that PIAs should be done whenever a new information system or communication technology is considered, regardless of whether this falls under the HIA.

The goal of a PIA is to:

- identify the privacy risks related to the project and potential mitigation measures;
- assess the privacy risks and mitigation measures identified;
- ensure that privacy principles and legislation are considered and adhered to;
- promote decision-making that takes privacy awareness into consideration;
- document, mitigate, and manage privacy related risks identified.

## **PIA COMPONENTS:**

### **PART 1 – GENERAL**

- Provides a broad overview about the project and assessment of what type of information is involved.

### **PART 2 – PRIVACY ENVIRONMENTAL ASSESSMENT**

- Provides an overview of safeguards and how information will be managed and protected.

### **PART 3 – PRIVACY RISK ANALYSIS**

- Provides an overview on information flow mapping, significant risks, and mitigation strategies.

### **PART 4 – FURTHER INFORMATION**

- Provides supporting information to assist decision-makers.

### **PART 5 – SIGNATURES AND APPROVALS**

- Provides a record of approval.

*Instructions: In following sections delete the descriptive text (in italics) and replace it with your own. Complete the entire form, attach any relevant documents and route in hard copy or via email.*

## PART 1 - GENERAL

### Project Description

<b>1. Provide description of project:</b>
<p><i>Describe.</i></p> <ul style="list-style-type: none"> <li>• <i>Rationale, purpose and objectives;</i></li> <li>• <i>Project lead or sponsor;</i></li> <li>• <i>Any links with existing programs or services, etc.;</i></li> <li>• <i>Clearly indicate if this is a <u>new</u> project or <u>change to an existing approved</u> project;</i></li> <li>• <i>If the project involves modifications to an existing program or service, first describe the existing program or service and the proposed changes;</i></li> <li>• <i>Scope;</i></li> <li>• <i>Key project deadlines, milestones;</i></li> <li>• <i>Funding / Budget of project.</i></li> </ul>
<b>2. If applicable, provide information of any prior PIA completed in relation to the project:</b>
<ul style="list-style-type: none"> <li>• <i>Attach copy of past PIA</i></li> </ul>

### Authority and Context

<b>3. Identify accountable party(s):</b> <i>"Accountable party" refers to an organization/party who is ultimately accountable for the project. E.g. project sponsors, decision-makers, those with statutory authority.</i>
<i>List organization(s):</i>
<b>4. What legislative authority do you have to collect, use, or disclose the information related to this project?</b>
<p><i>Describe:</i></p> <ul style="list-style-type: none"> <li>• <i>The authority under which the information is being collected, used, or disclosed.</i></li> <li>• <i>Cite legislation (sections and provisions).</i></li> <li>• <i>Explain why your project falls into the scope of that authority.</i></li> </ul>

### Information Involved

<b>5. What elements of information or data are involved in the project?</b>
<p><i>Should address:</i></p> <ul style="list-style-type: none"> <li>• <i>Client information;</i></li> <li>• <i>Employee information;</i></li> <li>• <i>Financial information;</i></li> <li>• <i>Any other type of information involved.</i></li> </ul>
<b>6. What is the source of the information being collected and stored?</b>
<p><i>Describe the source.</i> <i>E.g. patients, the general public, other information systems, third party organizations, etc.</i></p>
<b>7. How is the information being collected?</b>
<p><i>Describe the method.</i> <i>E.g. from patients themselves, interviews, surveys, forms, etc.</i></p>

8. Does the project involve the collection, use, or disclosure of personal information and/or personal health information?	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
Describe. (Also include description of how the information is identifiable or non-identifiable).	
9. What is the information being used for?	
Describe (if applicable).	
10. Does the project involve personal information and/or personal health information that once collected for a particular purpose will be used or disclosed for another purpose(s)?	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
Describe if the information will be used for e.g. for business planning, system planning and disclosed to whom, and why.	
11. When legislative authority allows, will personal information or personal health information collected or used in the project be disclosed to external third parties? (E.g. Chief Electoral Officer, CIHI, Statistics Canada)	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
Describe.	
12. Does the project change or affect how personal information and/or personal health information is currently stored, secured, or retained?	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
13. Will the project change the approach by which personal information and/or personal health information already held is disclosed?	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
14. Will the project affect an individual's access to their own information?	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
Describe.	
15. Is collection, use, and/or disclosure of personal information and/or personal health information occurring without the individual's consent?	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
Describe.	
16. How is the information being disclosed/shared?	
Describe and attach copy of an agreement, if relevant.	

<i>E.g. allowed based on a current agreement.</i>	
<p>17. Does the project link to an “integrated program or activity”, which involves more than one type of personal information and/or personal health information held by more than one program area/Department?  <i>E.g. education and health, child protection and health, justice and mental health. Department of Justice and Department of Education, Culture and Employment's work on integrated case are examples of “integrated programs or services”.</i></p>	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
Describe.	
<p>18. Will the project involve the collection, use, disclosure, or storage of personal information or personal health information outside of the NWT?</p>	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
Describe.	
<p>19. As a part of the project will personal information and/or personal health information be collected/used by contractors and/or disclosed to contractors?</p>	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
Describe.	

**CHECK POINT:** If you answered YES to any of the questions in Part 1 - move to next page and complete Parts 2-5 of the PIA.

If you answered NO to all YES/NO questions in Part 1 - move to Part 5 and complete Part 5 of the PIA.

## PART 2 – PRIVACY ENVIRONMENTAL ASSESSMENT

### Maintaining Information – Privacy Protection, Security, Accuracy, Correction

<b>20. Of the following what privacy and security safeguard measures <u>are</u> documented and <u>in</u> place to reduce the risk of a privacy breach?</b>	
<i>Describe all safeguards in place to protect the information.</i> <ul style="list-style-type: none"> <li>• Administrative safeguards: (E.g. any specific policies, procedures, agreements, and directives used to protect privacy)</li> <li>• Technical safeguards: (E.g. computer/software-related safeguards like encryption, passwords, electronic tracking, automatic log-offs, etc.)</li> <li>• Physical safeguards: (E.g. locked cabinets, restricted areas)</li> </ul>	
<b>21. What particular privacy and security safeguard measures are documented and in place if sharing information outside of the NWT?</b>	
<i>Describe.</i>	
<b>22. How is data integrity maintained?</b>	
<i>Describe what is in place to ensure the information is kept accurate and up-to date. If information is not updated explain how the project will ensure the information involved is accurate.</i>	
<b>23. What legislative authority governs the privacy and security safeguard measures that <u>must be in place</u>?</b>	
<i>Document here the authority. Cite legislation (sections and provisions).</i>	
<b>24. What policies govern the privacy and security safeguard measures that <u>must be in place</u>?</b>	
<i>List all applicable policies.</i>	
<b>25. What capacity does the project have for controlling who has access to the personal information and/or personal health information involved?</b>	
<i>If it is an information system/communication technology, describe the capacity already built into the system/technology; <u>OR</u></i> <i>If this is another type of project, describe what inherently is in place to restrict access to personal information and/or personal health information.</i>	
<b>26. What access control methods/best practices (e.g. auditing/RBAC, unique sign-on) will be put in place in addition to pre-existing controls covered above?</b>	
<i>Describe.</i>	N/A <input type="checkbox"/>
<b>27. Will all users of the system / all those involved in the project be trained in privacy and be familiar with relevant privacy/security policies, procedures, standards and safeguard measures?</b>	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
<i>If yes, describe how.</i>	

28. Will identifiable information be de-identified ? <i>"De-identification" means process to remove details from information that make it possible to recognize which particular person the information is connected with.</i>	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
<i>If yes, describe the method of de-identification to be used. Describe the approach and explain how it is compliant with applicable legislative requirements for de-identification.</i>	
29. What mitigation measures are in place to prevent/reduce the risk of re-identification?	
<i>Describe.</i>	
30. Is there sufficient/dedicated funding allocated to support the project/system overall?	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
<i>Describe and identify the funding specifically to address privacy and security aspects of the project.</i>	
31. Overall do the project and project outcomes inherently adhere to privacy best practices? ( <i>"Privacy by Design" – not incorporating privacy practices after the fact</i> )	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
32. Does the project/system meet the below privacy principles? Basic privacy principles:	
<ul style="list-style-type: none"> <li>• Collect, use, and disclose the least amount of information, and on a need-to-know basis</li> <li>• Collect, use, and disclose de-identified information unless identifiable information is necessary</li> </ul>	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
<i>Describe the details.</i>	
33. Is there additional/other information about the project relevant to PART 2-Privacy Environmental Assessment?	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
<i>Describe.</i>	



### PART 3 – PRIVACY RISK ANALYSIS

The Privacy Risk Analysis includes the following components:

- Mapping the Flow of Information
- Privacy Risk Identification
- Privacy Risk Map
- Risk Mitigation Identification

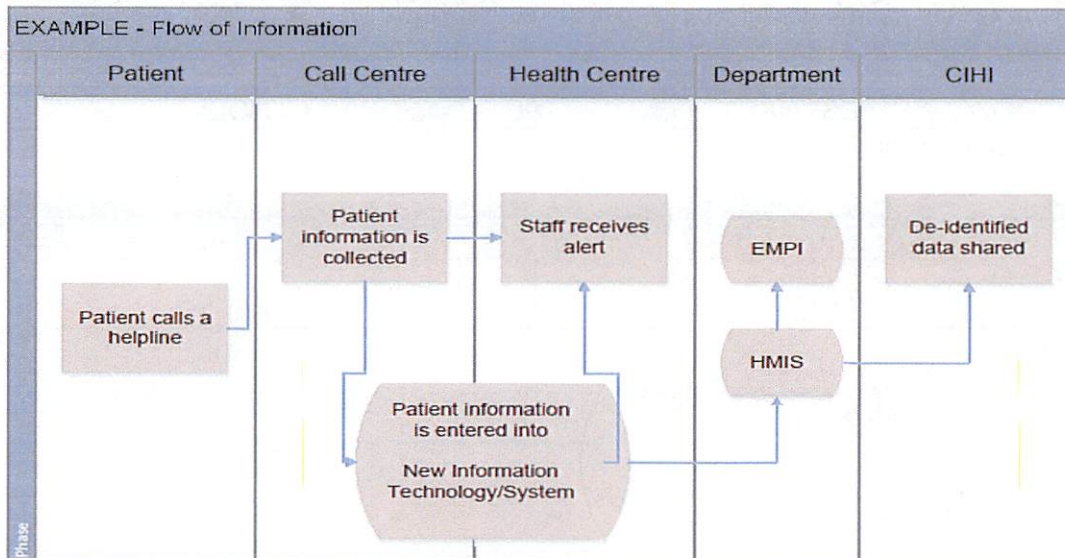
*Feel free to add additional documents, as they become relevant, to provide a full understanding of the level of privacy risk and impact to individuals.*

#### Mapping the Flow of Information

34. Provide a flow of information.

*Capture the flow of information using a table or flow chart to illustrate how information will be collected, used, and disclosed as a part of the project. The table or flow chart should capture how information moves (collected, used, disclosed, transmitted or exchanged) and include a reference to the related legislative authority. The examples below can be replaced with the project specific table or flowchart.*

Example flowchart:



**Example Flow Table:****Personal Information Flow Table**

	Description/Purpose	Type of Action	Legislative Authority
1.	Personal health information entered into electronic health information system	Disclosure	HIA s. 63
2.	De-identified personal health information forwarded to CIHI	Disclosure	HIA s. 61

**Privacy Risk Identification**

35. Identify the privacy risks associated with the project.

Use the table and legends below to identify privacy risks associated with the project. Identify the likelihood of this risk happening and the level of impact it would have on individuals if it occurred. See legends under the table for likelihood and impact criteria. The example (R1) can be removed and additional lines added as needed.

**Example table**

Risk ID	Privacy Risk	Threat Scenario	Current Safeguards	Vulnerabilities	Impact	Likelihood
<b>Example R1</b>	Unauthorized Collection	Collection of personal health information without consent	Control over collection of information described	Method for addressing unauthorized collection not completely applied	2	D

**Legend: Likelihood Criteria**

Likelihood Criteria	
A	Event has occurred in the last 3 months and likelihood to happen in the next 3 to 5 years is high (>75%)
B	Event has occurred in the last 6 months and it could happen again in the next 3 to 5 years (50%-75%)
C	Has occurred in the last 12 months and likelihood to happen in the next 3 to 5 years is moderate (25-50%)
D	Has occurred in the last 3 years and the likelihood of it happening is moderate (not higher than 25%)
E	Has not happened in the last 5 years and is not likely to occur in the next 3 to 5 years (<10%)



## Legend: Impact Level

Impact Level	Infrastructure	Information	Programs & Services	Client & Public
	<i>Refers to buildings, work space, equipment, power, water</i>	<i>Refers to various ways we communicate and create, transmit and store information</i>	<i>Refers to everything that directly relates to programs and services</i>	<i>Refers to clients (patients) and public, overall those who we need a strong relationship with.</i>
5 Extreme	<ul style="list-style-type: none"> <li>Loss of key physical assets</li> <li>Significant increase/decrease in federal funding</li> <li>Irreparable, significant damage to environment</li> <li>Long term impact or closure of facility</li> </ul>	<ul style="list-style-type: none"> <li>Exposure of critical confidential information</li> <li>Business and clinical software or databases not available indefinitely</li> <li>Records/data not accessible compromising care and operations</li> <li>Radical reportable and actionable privacy breach</li> </ul>	<ul style="list-style-type: none"> <li>Total loss of service or program</li> <li>Unable to perform essential services for extended period</li> <li>Ability to deliver newly identified essential services</li> <li>Loss of operational license</li> </ul>	<ul style="list-style-type: none"> <li>Loss of client/public confidence resulting in long-term or permanent loss of reputation and clients' trust in services</li> <li>Public/media outcry for changes in administration and Minister</li> <li>Very positive/negative public ratings</li> </ul>
4 Major	<ul style="list-style-type: none"> <li>Loss of significant physical assets</li> <li>Major environmental damage – extended clean-up required/some permanent damage</li> <li>Short-term issue with impact to operations</li> </ul>	<ul style="list-style-type: none"> <li>Exposure of significant amount of confidential information</li> <li>Business and clinical software or databases not available for long-term</li> <li>Major delay with access to records/data impacting client</li> <li>Reportable privacy breach</li> </ul>	<ul style="list-style-type: none"> <li>Significant gain/loss of service or program</li> <li>Significant improvements/disruption in delivery of essential services</li> <li>Significant over / under achievement of service/program objectives</li> <li>Loss of accreditation</li> </ul>	<ul style="list-style-type: none"> <li>Major gain/loss of client and public trust</li> <li>Public/media outcry for removal of departmental official</li> <li>Major praise/criticism by external/internal audit</li> </ul>
3 Moderate	<ul style="list-style-type: none"> <li>Loss of large, but replaceable physical assets</li> <li>Moderate environmental damage with moderate clean-up effort, no permanent damage</li> <li>Moderate issue with impact to operations</li> </ul>	<ul style="list-style-type: none"> <li>Exposure of limited amount of confidential sensitive information</li> <li>Business and clinical software or databases not available for moderate term</li> <li>Significant delay with access to records/data</li> <li>Isolated privacy breach</li> </ul>	<ul style="list-style-type: none"> <li>Moderate gain/loss of service</li> <li>Moderate improvements/disruptions in essential services</li> <li>Moderate over / under achievement of service/program objectives</li> <li>Temporary revocation of accreditation</li> </ul>	<ul style="list-style-type: none"> <li>Moderate gain/loss of client and public trust</li> <li>Positive/negative national media attention</li> <li>Moderate recommendations from external or internal audit</li> </ul>
2 Minor	<ul style="list-style-type: none"> <li>Limited loss of physical assets</li> <li>Minor, non-permanent damage requiring very limited clean-up efforts</li> <li>Minor issue with minimal impact to operations</li> </ul>	<ul style="list-style-type: none"> <li>Limited exposure of sensitive information</li> <li>Business and clinical software or database not available for short term</li> <li>Delayed access to records/data</li> <li>No privacy breach</li> </ul>	<ul style="list-style-type: none"> <li>Limited gain/loss of service</li> <li>Minor improvements/disruption in services, projects or processes</li> <li>Minor gain/setbacks in achievement of service/program objectives</li> <li>Remediation of issue related to accreditation or operational license</li> </ul>	<ul style="list-style-type: none"> <li>Minor gain/setbacks in building client and public trust</li> <li>Some favorable/unfavorable local media attention</li> <li>Minimal improvements suggested by external or internal audit</li> </ul>
1 Insignificant	<ul style="list-style-type: none"> <li>Very limited loss of physical assets</li> <li>Very minor, non-permanent environmental damage requiring no clean-up measures</li> <li>No impact to operations</li> </ul>	<ul style="list-style-type: none"> <li>Very limited exposure of sensitive information</li> <li>Non-critical software or databases unavailable for a limited period</li> <li>Limited impact in accessing records/data</li> <li>No privacy breach</li> </ul>	<ul style="list-style-type: none"> <li>No or very minor gain/loss of service data</li> <li>No or very minor improvement in services, programs or processes</li> <li>No issues with accreditation or operational license</li> </ul>	<ul style="list-style-type: none"> <li>No or very minor impact on client/public trust</li> <li>No or very minor media attention</li> </ul>

### Privacy Risk Map

36. Map the privacy risks associated with the project.

Use the map below and place individual risks identified earlier in the Privacy Risk Identification using the Likelihood (A-E) and Impact (1-5) that correspond with the risks.

Likelihood	Impact					
		1 Insignificant	2 Minor	3 Moderate	4 Major	5 Extreme
	A Almost Certain	M	M	M-H	H	H
	B Likely	L-M	M	M-H	H	H
	C Possible	L	L-M	M	M-H	H
	D Unlikely	L	L <b>R1</b>	L-M	M	M-H
	E Rare	L	L	L-M	L-M	M

### Risk Mitigation Identification

37. Identify and describe the mitigation measures that will be put in place to address the risks identified.

Use the table below to describe the mitigation measures that will be implemented for the risks identified earlier. Identify the parties responsible for each mitigation measure.

Use the legend below the table to identify what project privacy risks must be mitigated.

Risk Mitigation Table				
Risk ID	Privacy Risk	Risk Level	Mitigation Measures	Responsible Party/Lead
R1.	Example: Employees could access personal information inappropriately without authorization.	L	• Oath of Employment	• DHSS
			• Role based access control	• DHSS, HPU
			• Training	• YHSSA
R2.	...		• ...	• ...



## Legend: Recommended Actions for Identified Risks

	Description	Action	Mitigation planning
Must be addressed	High Risk	Must be addressed by Senior Management through a detailed review and detailed plans.	High Risk and Moderate to High Risk must be mitigated <u>before</u> a project may be approved. Mitigation measures must be set out formally and implemented on a continual basis for as long as <i>high risk</i> and <i>moderate to high risk</i> level naturally occurs.
	Moderate to High Risk	Requires review and planning by Senior Management.	
Acceptable	Moderate Risk	Can be addressed through specific allocation of management responsibility, specific monitoring and response procedures.	
	Low to Moderate Risk	Can be addressed through specific monitoring, or response procedures.	
	Low Risk	Can be managed by routine procedures.	

38. Is there dedicated permanent funding identified specifically to implement the mitigation measures?		
YES <input type="checkbox"/>	NO <input type="checkbox"/>	N/A <input type="checkbox"/>
Describe the details.		
39. What arrangements have been made to implement the mitigation measures?		
Describe the details.		N/A <input type="checkbox"/>
40. What arrangements have been made to monitor and evaluate the effectiveness of the identified mitigation measures?		
Describe the details.		N/A <input type="checkbox"/>
41. What ability is there to adjust the mitigation measures if they are found to be insufficient?		
Describe the details.		N/A <input type="checkbox"/>

#### PART 4 – FURTHER INFORMATION

42. Explain how the project supports current HSS priorities.	
<i>Describe the details.</i>	
43. Explain how the project aligns with GNWT Information and Communications Technology (ICT) strategy and system priorities.	
<i>Describe the details.</i>	N/A <input type="checkbox"/>
44. Explain how the project outcomes contribute to the sustainability of the HSS system.	
<i>Describe the details.</i>	
45. Do you have any other comments or information with respect to the above (PART 1-4)?	
YES <input type="checkbox"/>	NO <input type="checkbox"/>
<i>If Yes, describe here and attach any additional document you think are relevant  E.g. request for proposal, contract, budget, policy, organizational chart, job description, terms of reference, etc.</i>	

## PART 5 – SIGNATURES AND APPROVAL

☐ **Department of Health and Social Services Approval Routing**

The approval of this PIA is based on a review of the material provided. Any future changes to the scope of this project require an updated PIA to be submitted and approved.

_____ Project Manager	_____ Signature	_____ Date
_____ Director Responsible for Project/ Project Lead Director	_____ Signature	_____ Date
_____ Director, Finance	_____ Signature	_____ Date
_____ Director, Information Services	_____ Signature	_____ Date
_____ Chief Health Privacy Officer	_____ Signature	_____ Date
_____ Director, Policy, Legislation and Communications	_____ Signature	_____ Date
_____ Assistant Deputy Minister, Corporate Services	_____ Signature	_____ Date
_____ Deputy Minister, Health and Social Services	_____ Signature	_____ Date

Note: If PIA identifies multiple accountable parties (see PART 1 #3), the appropriate senior level representative from each party must approve the PIA. Add additional signature lines as required:

_____ Name	_____ Signature	_____ Date
_____ Title		
_____ Organization		

COMPLETION OF THE ABOVE SIGNALS THE OVERALL

COMPLETION AND ACCEPTANCE OF THIS PIA.

A copy of this PIA has been sent to the NWT Information and Privacy Commissioner by

\_\_\_\_\_  
Name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date Sent

\_\_\_\_\_  
Title

☐

The approval of this PIA is based on a review of the material provided. Any future changes to the scope of this project require an updated PIA to be submitted and approved.

Date \_\_\_\_\_

Date \_\_\_\_\_

Date \_\_\_\_\_

Date \_\_\_\_\_

Date \_\_\_\_\_

Date \_\_\_\_\_

Date \_\_\_\_\_

**Note: If PIA identifies multiple accountable parties (see PART 1 #3), the appropriate senior level representative from each party must approve the PIA. Add additional signature lines as required:**

Date \_\_\_\_\_

## Organization

COMPLETION OF THE ABOVE SIGNALS THE OVERALL

COMPLETION AND ACCEPTANCE OF THIS PIA.

A copy of this PIA has been sent to the NWT Information and Privacy Commissioner by

\_\_\_\_\_  
Name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date Sent

\_\_\_\_\_  
Title