



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.

<original signed by>

Deputy Minister

May 3, 2017

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 I 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 I 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 I HSSA must ensure employees cooperate during an initial review and full investigation.

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

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

The Department I 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 I 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 OM 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 I 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.