



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

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

<original signed by>

Deputy Minister

May 3, 2017

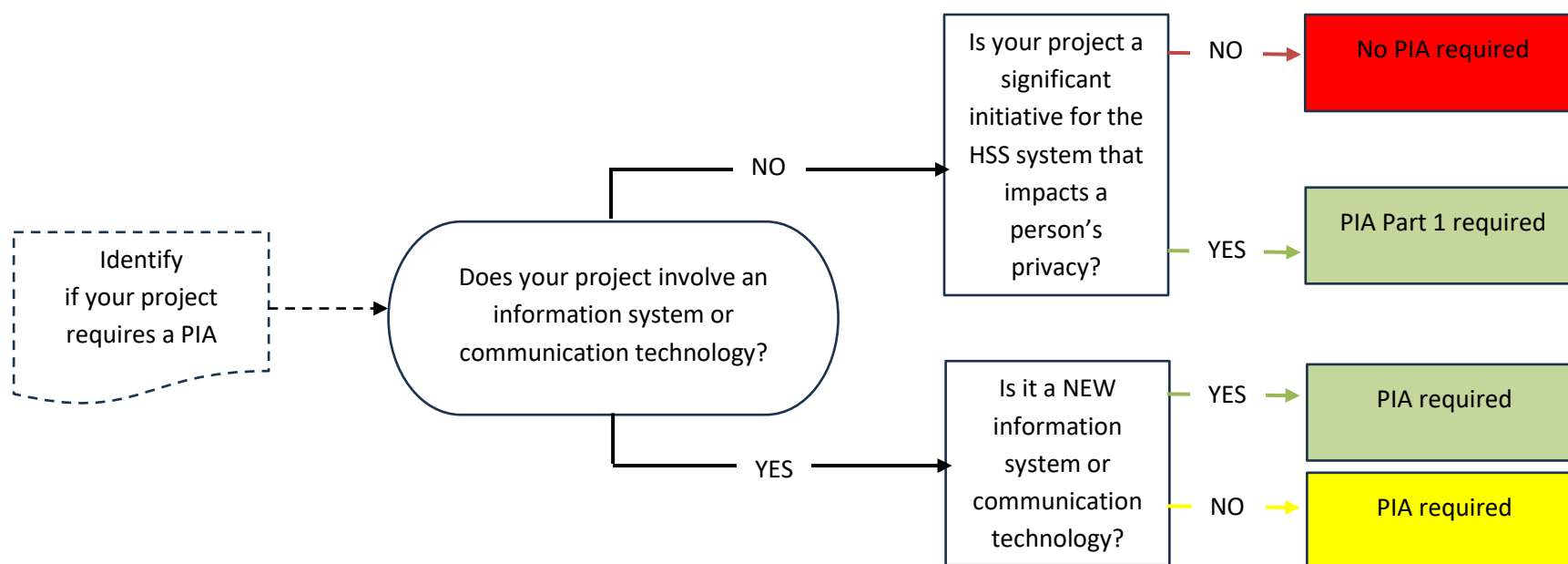
Date

APPENDIX 1

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

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.



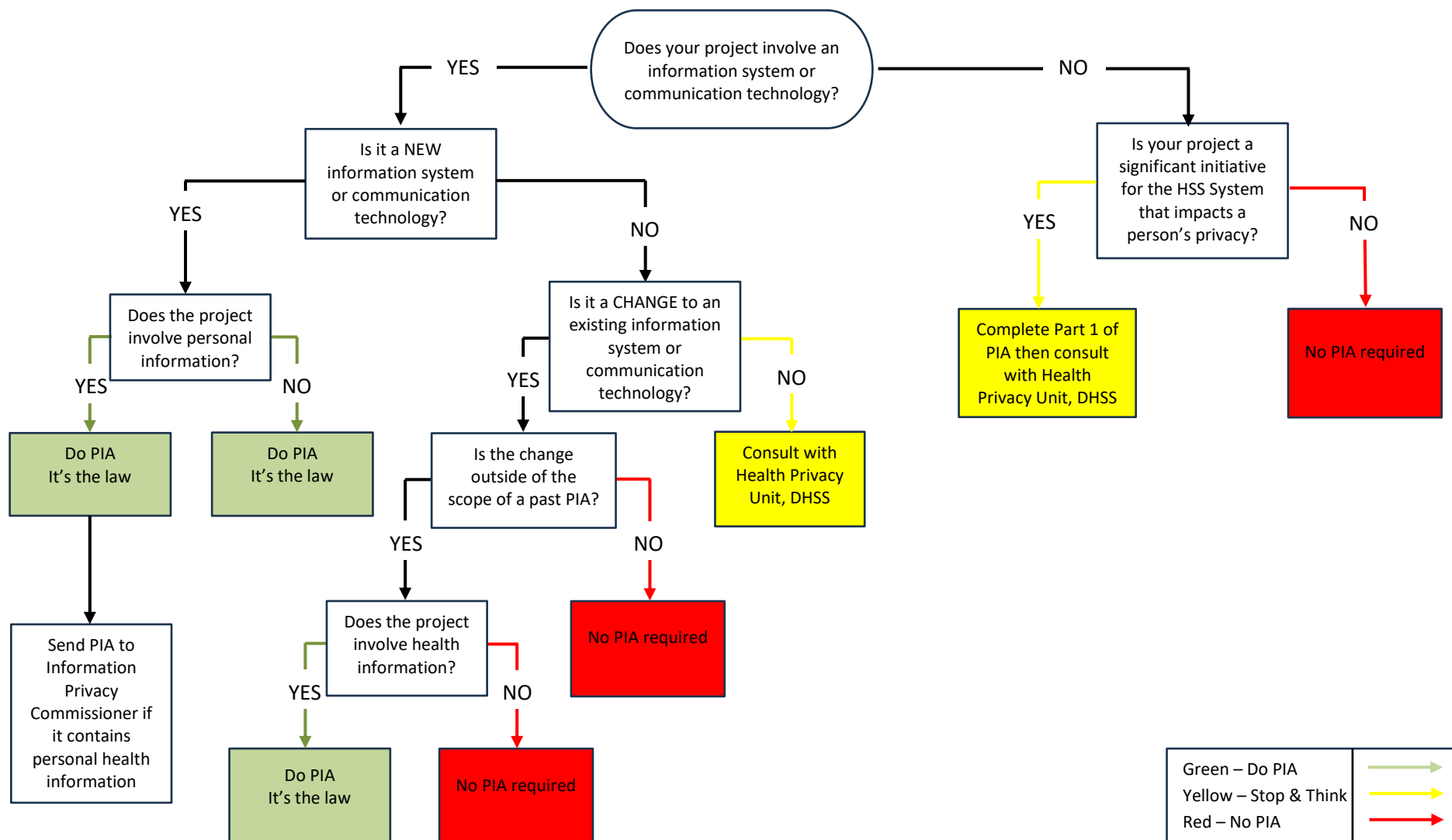
Conducting a PIA ensures a compliance with Northwest Territories laws and regulations governing privacy and demonstrates Territorial HSS system's commitment to protect the privacy of residents/clients.

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



Privacy Impact Assessment (PIA) DECISION TREE

For Territorial Health and Social Services (HSS) Projects



APPENDIX 2

PRIVACY IMPACT ASSESSMENT

Submit PIA to:	Health Privacy Unit Information Services Department of Health and Social Services Government of the Northwest Territories HIA@gov.nt.ca / 867-767-9052 OR 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.

Project Description

1. Provide description of project:
<i>Describe.</i> <i>Rationale, purpose and objectives;</i> <i>Project lead or sponsor;</i> <i>Any links with existing programs or services, etc.;</i> <i>Clearly indicate if this is a <u>new project</u> or <u>change to an existing approved project</u>;</i> <i>If the project involves modifications to an existing program or service, first describe the existing program or service and the proposed changes;</i> <i>Scope;</i> <i>Key project deadlines, milestones;</i> <i>Funding / Budget of project.</i>
2. If applicable, provide information of any prior PIA completed in relation to the project:
<i>Attach copy of past PIA</i>

Authority and Context

3. Identify accountable party(s): <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>
4. What legislative authority do you have to collect, use, or disclose the information related to this project?
<i>Describe:</i> <i>The authority under which the information is being collected, used, or disclosed.</i> <i>Cite legislation (sections and provisions).</i> <i>Explain why your project falls into the scope of that authority.</i>

Information Involved

5. What elements of information or data are involved in the project?
<i>Should address:</i> <i>Client information;</i> <i>Employee information;</i> <i>Financial information;</i> <i>Any other type of information involved.</i>
6. What is the source of the information being collected and stored?
<i>Describe the source.</i> <i>E.g. patients, the general public, other information systems, third party organizations, etc.</i>

7. How is the information being collected?	
<i>Describe the method.</i> <i>E.g. from patients themselves, interviews, surveys, forms, etc.</i>	
8. Does the project involve the collection, use, or disclosure of personal information and/or personal health information?	
YES ☐	NO ☐
<i>Describe.</i> <i>(Also include description of how the information is identifiable or non-identifiable).</i>	
9. What is the information being used for?	
<i>Describe (if applicable).</i>	
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 ☐	NO ☐
<i>Describe if the information will be used for e.g. for business planning, system planning and disclosed to whom, and why.</i>	
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 ☐	NO ☐
<i>Describe.</i>	
12. Does the project change or affect how personal information and/or personal health information is currently stored, secured, or retained?	
YES ☐	NO ☐
13. Will the project change the approach by which personal information and/or personal health information already held is disclosed?	
YES ☐	NO ☐
14. Will the project affect an individual's access to their own information?	
YES ☐	NO ☐
<i>Describe.</i>	
15. Is collection, use, and/or disclosure of personal information and/or personal health information occurring without the individual's consent?	
YES ☐	NO ☐
<i>Describe.</i>	

16. How is the information being disclosed/shared?	
<i>Describe and attach copy of an agreement, if relevant. E.g. allowed based on a current agreement.</i>	
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>	
YES ☐	NO ☐
<i>Describe.</i>	
18. Will the project involve the collection, use, disclosure, or storage of personal information or personal health information outside of the NWT?	
YES ☐	NO ☐
<i>Describe.</i>	
19. As a part of the project will personal information and/or personal health information be collected/used <u>by</u> contractors and/or disclosed <u>to</u> contractors?	
YES ☐	NO ☐
<i>Describe.</i>	

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

20. Of the following what privacy and security safeguard measures <u>are</u> documented and <u>in place</u> to reduce the risk of a privacy breach?	
<i>Describe all safeguards in place to protect the information.</i> - Administrative safeguards: (E.g. any specific policies, procedures, agreements, and directives used to protect privacy) - Technical safeguards: (E.g. computer/software-related safeguards like encryption, passwords, electronic tracking, automatic log-offs, etc.) - Physical safeguards: (E.g. locked cabinets, restricted areas)	
21. What particular privacy and security safeguard measures are documented and in place if sharing information outside of the NWT?	
<i>Describe.</i>	
22. How is data integrity maintained?	
<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>	
23. What legislative authority governs the privacy and security safeguard measures that <u>must be in place</u> ?	
<i>Document here the authority. Cite legislation (sections and provisions).</i>	
24. What policies govern the privacy and security safeguard measures that <u>must be in place</u> ?	
<i>List all applicable policies.</i>	
25. What capacity does the project have for controlling who has access to the personal information and/or personal health information involved?	
<i>If it is an information system/communication technology, describe the capacity already built into the system/technology; <u>OR</u> 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>	
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?	
<i>Describe.</i>	N/A ☐
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?	
YES ☐	NO ☐
<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 ☐	NO ☐
<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 ☐	NO ☐
<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 ☐	NO ☐
32. Does the project/system meet the below privacy principles? Basic privacy principles:	
• Collect, use, and disclose the least amount of information, and on a need-to-know basis • Collect, use, and disclose de-identified information unless identifiable information is necessary	
YES ☐	NO ☐
<i>Describe the details.</i>	
33. Is there additional/other information about the project relevant to PART 2-Privacy Environmental Assessment?	
YES ☐	NO ☐
<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

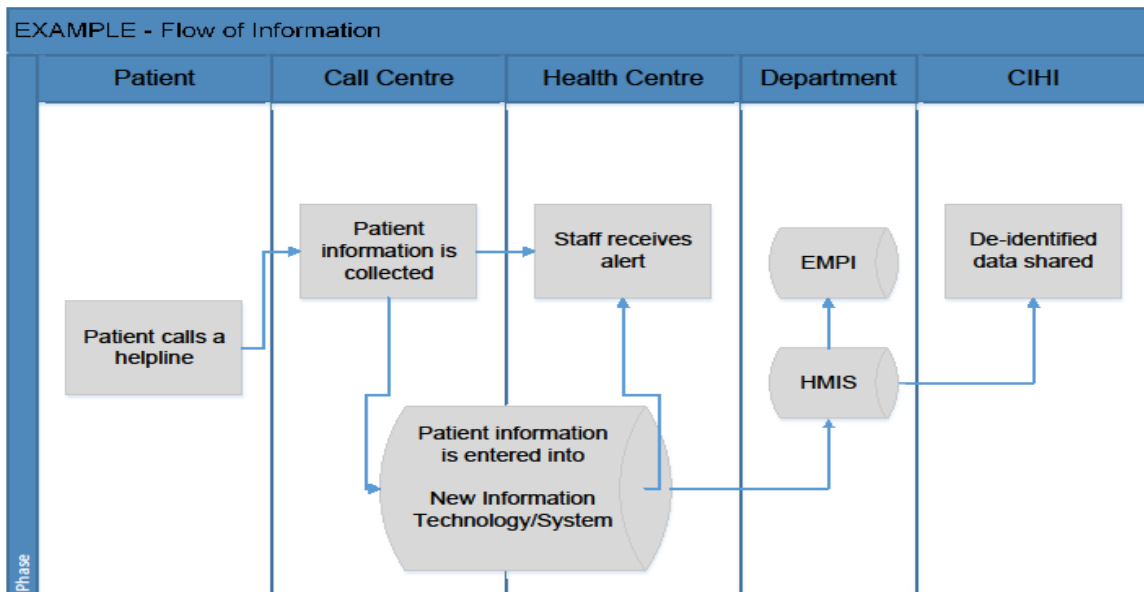
Feel free to add additional documents, as they become relevant, to provide a full understanding of the level of privacy risk and impact to individuals.

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
Example R1	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%)

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	- Loss of key physical assets - Significant increase/decrease in federal funding - Irreparable, significant damage to environment - Long term impact or closure of facility	- Exposure of critical confidential information - Business and clinical software or databases not available indefinitely - Records/data not accessible compromising care and operations - Radical reportable and actionable privacy breach	- Total loss of service or program - Unable to perform essential services for extended period - Ability to deliver newly identified essential services - Loss of operational license	- Loss of client/public confidence resulting in long-term or permanent loss of reputation and clients' trust in services - Public/media outcry for changes in administration and Minister - Very positive/negative public ratings
4 Major	- Loss of significant physical assets - Major environmental damage – extended clean-up required/some permanent damage - Short-term issue with impact to operations	- Exposure of significant amount of confidential information - Business and clinical software or databases not available for long-term - Major delay with access to records/data impacting client - Reportable privacy breach	- Significant gain/loss of service or program - Significant improvements/disruption in delivery of essential services - Significant over / under achievement of service/program objectives - Loss of accreditation	- Major gain/loss of client and public trust - Public/media outcry for removal of departmental official - Major praise/criticism by external/internal audit
3 Moderate	- Loss of large, but replaceable physical assets - Moderate environmental damage with moderate clean-up effort, no permanent damage - Moderate issue with impact to operations	- Exposure of limited amount of confidential sensitive information - Business and clinical software or databases not available for moderate term - Significant delay with access to records/data - Isolated privacy breach	- Moderate gain/loss of service - Moderate improvements/disruptions in essential services - Moderate over / under achievement of service/program objectives - Temporary revocation of accreditation	- Moderate gain/loss of client and public trust - Positive/negative national media attention - Moderate recommendations from external or internal audit
2 Minor	- Limited loss of physical assets - Minor, non-permanent damage requiring very limited clean-up efforts - Minor issue with minimal impact to operations	- Limited exposure of sensitive information - Business and clinical software or database not available for short term - Delayed access to records/data - No privacy breach	- Limited gain/loss of service - Minor improvements/disruption in services, projects or processes - Minor gain/setbacks in achievement of service/program objectives - Remediation of issue related to accreditation or operational license	- Minor gain/setbacks in building client and public trust - Some favorable/unfavorable local media attention - Minimal improvements suggested by external or internal audit
1 Insignificant	- Very limited loss of physical assets - Very minor, non-permanent environmental damage requiring no clean-up measures - No impact to operations	- Very limited exposure of sensitive information - Non-critical software or databases unavailable for a limited period - Limited impact in accessing records/data - No privacy breach	- No or very minor gain/loss of service data - No or very minor improvement in services, programs or processes - No issues with accreditation or operational license	- No or very minor impact on client/public trust - No or very minor media attention

Legend: Impact Level

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 R1	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	L	• Oath of Employment	• DHSS
			• Role based access control	• DHSS, HPU

	<i>information inappropriately without authorization.</i>		• <i>Training</i>	• <i>YHSSA</i>
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.	<i>High Risk and Moderate to High Risk must be mitigated <u>before</u> a project may be approved.</i> 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 ☐	NO ☐	N/A ☐
Describe the details.		
39. What arrangements have been made to implement the mitigation measures?		
Describe the details.		N/A ☐
40. What arrangements have been made to monitor and evaluate the effectiveness of the identified mitigation measures?		
Describe the details.		N/A ☐
41. What ability is there to adjust the mitigation measures if they are found to be insufficient?		
Describe the details.		N/A ☐

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 ☐
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 ☐	NO ☐
<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

☐ **Health and Social Service Authority 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, Quality, Safety and Client Experience /Director resp.for Quality and Risk	_____ Signature	_____ Date
--	--------------------	---------------

_____ Chief Health Privacy Officer, DHSS	_____ Signature	_____ Date
---	--------------------	---------------

_____ Executive Director, Corporate Services /Director resp. for Finance	_____ Signature	_____ Date
--	--------------------	---------------

_____ Director ISSC /Director resp. for Information Services	_____ Signature	_____ Date
--	--------------------	---------------

_____ Chief Executive Officer, Health and Social Services Authority	_____ 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

DATE (mm/dd/yyyy)

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