Health PEI Santé Î.-P.-É.

IMPORTANT NOTE: The Policy Document Management System (PDMS) is the only authority for policy documents for Health PEI. Always refer to the PDMS for the most current version of this policy document. The currency or accuracy of any printed policy document cannot be guaranteed, even if printed previously from PDMS. Paper-based policy manuals are not recommended at any time.

FEEDBACK on this policy from Health PEI users may be sent to healthpeipolicy@ihis.org

Name: HPEI Privacy Impact Assessment (PIA) Protocol

Date/Time Generated: Jun 21, 2023 13:23	**Generated By:** health\cgllewellyn

Policy and Procedures Manual

Operational/Clinical Protocol

PRIVACY IMPACT ASSESSMENT (PIA)

Health PEI			PROTOCOL
Applies To:	All Health PEI Healthcare workers		
Monitoring:	Privacy Officer		
Approving Authority:	Chief Administrative Officer		
Date:	Effective:	January 27, 2023	
	Next Review:	**January 27, 2025**	

This is a CONTROLLED document. Any copies of this document appearing in paper form should always be checked against the electronic version prior to use.

1.0 PROTOCOL

1.1 Health PEI meets its obligations and duties as a custodian under the *Health Information Act* (HIA), including the protection of personal health information (PHI) in its custody and/or control.

1.2 As required by the HIA, Health PEI shall prepare a privacy impact assessment (PIA) and submit the assessment to the Commissioner for review and comment in the following situations:

(a) for the new collection, use or disclosure of personal health information or any significant change to the collection, use or disclosure of personal health information;

(b) for the creation of a personal health information system or personal health information communication technology or a significant modification to a personal health information system or personal health information communication technology; or

(c) if a custodian performs data matching with personal health information collected by it or with any personal health information held by another custodian or another person.

1.3 Health PEI Leadership shall assess all new or planned initiatives for the need to conduct a PIA, in collaboration with the Privacy Officer as required.

(a) For initiatives involving information technology, Health PEI Leadership shall consult with Information Technology Shared Services (ITSS) to determine if a Threat Risk Assessment (TRA) is required in addition to a PIA.

1.4 Healthcare workers shall complete or ensure completion of a PIA where required by the HIA, to meet Health PEI's legislated obligation and to proactively identify and mitigate risks to individual privacy associated with an initiative.

1.5 The Health PEI Chief Executive Officer (CEO) shall submit all mandatory PIAs to the Commissioner's office, prior to the implementation of the initiative at the subject of the PIA.

1.6 Completed PIAs shall not be shared with external parties without approval from a member of the Executive Leadership Team and/or CEO.

2.0 DEFINITIONS

Collection (of PHI):	Gathering, acquiring, receiving or obtaining personal health information from any source
Commissioner:	The PEI Information and Privacy Commissioner, who has a duty to monitor the administration of the *Health Information Act* and authority to review and comment on mandatory privacy impact assessments completed by custodians in compliance with the HIA
Data matching	As defined in the *Health Information Act*, the creation of individually identifying personal health information by combining individually identifying personal health information, de-identified personal health information or other information from 2 or more electronic databases or 2 or more electronic records, without the consent of the individuals to whom the information relates
Disclosure (of PHI):	Releasing or making available personal health information by healthcare workers to a party that is external to Health PEI
Healthcare workers:	All persons involved in providing care and/or services within Health PEI facilities and programs, which includes all employees (casual, permanent, temporary, full-time and part-time employees), physicians (salaried, fee-for-service, contract and locum), students, volunteers and contract workers
Initiative:	Broadly refers to a system, program, project, implementation or upgrade that is planned or undertaken by Health PEI
Personal Health Information (PHI):	As defined in the *Health Information Act*, identifying information about an individual in oral or recorded form that includes but is not limited to information related to: • the individual's physical or mental health, family history or genetic information; • the provision of health care to the individual; • a drug, device or product provided to the individual by prescription or other authorization of a health care provider; • payments or eligibility for health care; • donation of any body part or bodily substance; or • the identity of the individual's substitute decision maker or health care provider.
Privacy Impact Assessment (PIA):	A process to proactively assess an initiative that will involve the collection, use or disclosure of PHI to identify and address any risks to individual privacy.

Privacy Officer:	The Director of Privacy and Information Management serves as Privacy Officer for Health PEI. The Director may delegate or assign duties to the Access to Information and Privacy Analyst(s).
Use (of PHI):	Accessing, viewing, handling or copying personal health information
Vendor:	An external party that supplies or will supply Health PEI with services or product that involve the collection, use, disclosure, storage or management of PHI, e.g. software or communication technology providers

3.0 PURPOSE/SCOPE

3.1 The purpose of this protocol is to:

(a) direct Health PEI's compliance with the HIA as it relates to mandatory PIAs,

(b) clarify roles and accountability for the completion of PIAs, and

(c) promote a consistent approach to conducting PIAs on Health PEI initiatives.

3.2 The purposes of a PIA are to:

(a) proactively identify risks to individual privacy related to an initiative,

(b) ensure that privacy best practices are incorporated into the planning process for all initiatives,

(c) promote effective management of privacy risk, and

(d) support Health PEI Leadership in weighing the risks and benefits of a proposed initiative in the context of the privacy of personal health information

4.0 APPLICATION

This protocol applies to all initiatives planned or undertaken by Health PEI healthcare workers that involve the collection, use or disclosure of PHI in the custody and/or control of Health PEI and meet the criteria for a required PIA.

5.0 FUNCTIONALITY/PROCESS

5.1 Roles and responsibilities in the PIA process

(a) The CEO, as corporate head of Health PEI, has overall accountability for the organization's compliance with the *Health Information Act*, including the completion of PIAs and submission to the Commissioner when required.

(b) The Privacy Officer provides advice and guidance to Health PEI Leadership on the completion of PIAs, including but not limited to:

(i) ensuring PIA resources and education are available for healthcare workers,

(ii) assessing new or planned initiatives for mandatory PIAs using criteria outlined in the HIA in collaboration with Health PEI Leadership.

(iii) providing support and guidance to Health PEI Leadership and healthcare workers on the completion of the PIA process and/or template,

(iv) liaising with ITSS staff as required regarding the security of personal health information,

(v) conducting the risk assessment component of the PIA process (for PIAs completed internally) and providing support, guidance and recommendations on risk mitigation plans,

(vi) liaising with external consultants hired to conduct PIAs on initiatives, in collaboration with Health PEI Leadership, as applicable,

(vii) facilitating the PIA sign off process and submission by CEO to the Commissioner,

(viii) liaising with the Commissioner to answer questions, provide additional information and follow up on Commissioner feedback or recommendations,

(ix) retaining signed original PIAs in central privacy and access files,

(x) ensuring copies of signed PIAs are distributed to the Project Sponsor and others, as appropriate, and

(xi) maintaining a registry of completed PIAs, to include tracking of recommendations, follow up and revisions or updates to the PIAs.

(c) Health PEI Leadership, including Chief Officers, Executive Directors, Directors, Managers and Supervisors, are accountable for:

(i) ensuring compliance with the legal requirement for submission of PIAs to the Commissioner, when the criteria outlined in the HIA apply to initiatives within their respective programs or areas of responsibility,

(ii) ensuring healthcare workers are aware of the PIA process,

(iii) ensuring that healthcare workers consider the need for conducting a PIA as part of planning initiatives,

(iv) ensuring completion of the PIA by identifying the most appropriate PIA author and allocating time and resources as required,

(v) obtaining technical information required to complete the PIA template in collaboration with ITSS and vendor(s) as applicable,

(vi) ensuring appropriate risk mitigation plans are identified and implemented,

(vii) ensuring initiative stakeholders are informed and engaged appropriately in the PIA process,

(viii) signing off on the completed PIA as Project Sponsor where applicable, and

(ix) ensuring vendors involved in an initiative participate in the PIA process by providing information about their services or systems, when required.

5.2 Determining if a PIA is required

(a) See Appendix A – *Decision Tool – Is a PIA required?*

(b) Consider the following examples of initiatives that may require a PIA:

(i) a collection of a new type of PHI that has not been collected before,

(ii) implementation of a new software that transmits PHI outside of the Health network,

(iii) research projects using PHI from multiple custodians,

(iv) implementation of a new electronic medical record, or

(v) an upgrade to an existing electronic health information system that introduces new remote access using mobile devices.

(c) Consider the following examples of initiatives where a PIA is not likely required:

(i) office relocation, or

(ii) routine software upgrades.

(d) Vendors may also be required to independently conduct and submit a PIA to the Commissioner, if the criteria for a mandatory PIA outlined in the HIA apply to the vendor as a custodian of PHI.

5.3 Time frames for initiating and completing a PIA

(a) The most appropriate time to complete a PIA is after the Project Charter is completed and approved, the business requirements and major deliverables for the initiative have been identified, and before a detailed project plan has been developed (see Appendix B - *PIA Process Map*).

(b) If a PIA is initiated;

(iii) too early in the planning process, there may not be enough information known about the initiative to complete the PIA template, or

(iv) too late in the planning process, there may not be enough time for the Commissioner to review and comment. This could result in cost and resource implications if changes to the initiative are required late in the process in order to address risks and/or the Commissioner's recommendations.

(c) Submit the PIA to the Privacy Officer only once all question/answer sections of the template have been completed. Risk assessments cannot be conducted on incomplete information.

(d) Where submission to the Commissioner is required, a PIA must be completed and signed off by the Project Sponsor no later than **three weeks** before the initiative is scheduled to be implemented.

(e) Revisit the PIA on a regular basis as it is a living document and is dependent on the duration of the initiative and any recommendations or follow up items that require action.

5.4 Elements of a PIA (content & scope)

(a) Describe the initiative, specify how PHI will be collected, used and disclosed, and identify any risks to individual privacy.

(b) In addition to the above items, include:

(i) the legal authority for the collection, use and/or disclosure of PHI,

(ii) a list of all PHI data elements that will be involved and the rationale for each element,

(iii) a detailed description of the planned flow of PHI from collection through to disposal, in a diagram format if applicable,

(iv) an assessment of the initiative using the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information, commonly referred to as the 10 Privacy Principles (Appendix C),

(v) an assessment of risks to privacy associated with the initiative and framed on the 10 Privacy Principles,

(vi) appropriate risk mitigation plans to address each identified risk, and

(vii) sign off by the Project Sponsor and Privacy Officer.

(c) Include appendices as applicable, such as patient information materials, educational resources, consent forms and vendor agreements specific to the initiative.

(d) Clearly define the scope of a PIA appropriately. The PIA should assess the new or planned initiative and not existing programs, policies, procedures, etc.

(e) For large and/or complex initiatives, it is recommended that the PIA be conducted by an external consultant with expertise in privacy and security. It is not necessary for external consultants to utilize the Health PEI PIA template.

(f) If it is not feasible to contract out a PIA, Health PEI Leadership must ensure a PIA is conducted using the Health PEI PIA template (available from Privacy Officer or on the Staff Resource Centre).

5.5 Risk Mitigation Plans

(a) The objective of a PIA is not necessarily to eliminate privacy risks completely but rather to have reasonable measures in place to reduce the likelihood of an incident occurring or to reduce the impact if an incident were to occur. Develop the risk mitigation plan with this in mind.

(b) Common privacy risks associated with new initiatives can include the collection of more PHI than is required to achieve the objectives of the initiative, the potential for unauthorized access to PHI and a lack of adequate technical security measures.

(c) Risk mitigation plans typically involve new or enhanced safeguards that will be employed to lower the risk to privacy, including administrative, physical and technical safeguards. Measures that increase the detectability of privacy incidents can also be beneficial.

(d) Include the following in your risk mitigation plan; the resource responsible for implementing the plan, a target completion date and approval or sign-off by the initiative Steering Committee and/or the Project Sponsor.

5.6 Privacy review

If an initiative does not meet the criteria for a mandatory PIA as outlined in the HIA, privacy can be incorporated into the planning process by completing a privacy review (see Appendix D – Privacy Review). This will ensure the initiative complies with the *Health PEI Privacy and Protection of Personal Health Information Policy* and the *10 Privacy Principles*.

5.7 Access to completed PIAs

Completed PIAs may contain information that, if released publicly, could threaten the security of PHI and expose Health PEI to risk.

(a) Requests for access to completed PIAs should be directed to the *Freedom of Information and Protection of Privacy Act* (FOIPP) request process.

5.8 Threat Risk Assessments (TRA)

(a) TRA's analyze information technology systems to identify vulnerabilities, threats and risks to the information collected, stored and/or transmitted by the system.

(b) For initiatives involving implementation of or a significant upgrade to an electronic health information system, consultation with ITSS will be needed to determine if a TRA is required, in addition to a PIA.

6.0 MONITORING

6.1 The Privacy Officer is responsible for ensuring this protocol is reviewed every two years according to Health PEI's policy review cycle and standards.

6.2 The Privacy Officer monitors compliance with this protocol and makes recommendations for revision, as required.

7.0 REFERENCES

Related Documents

HPEI Privacy and Protection of Personal Health Information Policy
HPEI Enterprise Risk Management Policy
PEI *Health Information Act,* RSPEI 1988, c H-1.41

PEI *Freedom of Information and Protection of Privacy Act*, RSPEI 1988, c F-15.01

References

Office of the Privacy Commissioner of Canada, accessed 2020-03-06, *Expectations: OPC's Guide to the Privacy Impact Assessment Process* (https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/)

Treasury Board of Canada, accessed 2020-04-08, *Directive on Privacy Impact Assessments*, (https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=18308)

PEI Information and Privacy Commissioner, accessed 2023-01-12, *Privacy Impact Assessments for Custodians and Researchers*, (https://www.assembly.pe.ca/sites/www.assembly.pe.ca/files/AMENDED%20April%2013%2C%202021%20OIPC%20guideline%20re%20PIA_0.pdf)

Office of the Information and Privacy Commissioner of Alberta 2010, accessed 2020-04-08, *Privacy Impact Assessment Requirements,* (www.oipc.ab.ca/action-items/privacy-impact-assessments.aspx)

Appendices

8.0 STAKEHOLDER REVIEW

Group/Committee	Dates of Review
Risk Advisor, Quality and Safety Division	April/May 2022
Focus Group – Healthcare staff with experience writing PIAs	April/May 2022
Chief Operating Officer	April/May 2022
ITSS Chief Information Security Officer	April/May 2022
ITSS IT Consultant	April/May 2022

9.0 REVIEW HISTORY

Review Dates: _____ _____ _____

_____ _____ _____

Appendix A – Decision Tool – Is a PIA required?

The *Health Information Act* requires the completion of PIAs in the following situations:

> for the new collection, use or disclosure of personal health information or any significant change to the collection, use or disclosure of personal health information;
>
> for the creation of a personal health information system or personal health information communication technology or a significant modification to a personal health information system or personal health information communication technology; or
>
> if a custodian performs data matching with personal health information collected by it or with any personal health information held by another custodian or another person.

Step 1 – Determine if personal health information (PHI) is collected, used or disclosed

Questions to consider:

What is PHI?

Identifying information (i.e. including name and/or date of birth and/or PHN) about an individual in oral or recorded form that includes but is not limited to information related to:

- the individual's physical or mental health, family history or genetic information;
- the provision of health care to the individual;
- a drug, device or product provided to the individual by prescription or other authorization of a health care provider;
- payments or eligibility for health care;
- donation of any body part or bodily substance; or
- the identity of the individual's substitute decision maker or health care provider.

What activities are considered to constitute collection, use or disclosure?

Collection: gathering, acquiring, receiving or obtaining PHI from any source

Use: accessing, viewing, handling or copying PHI

Disclosure: releasing or making available PHI to a party that is external to Health PEI

Does the initiative involve the collection, use or disclosure of PHI?

YES:	NO:
Proceed to Step 2 ↓	PIA not mandatory. Consider privacy review, if applicable.

Step 2 – Determine if the collection, use or disclosure of PHI is new or significantly changed

Questions to consider:

Has your program/service always collected this PHI?

Has your program/service used and/or disclosed this PHI in similar ways in the past?

Are you using PHI for a purpose that you have not used it for previously?

Are new external parties accessing or receiving PHI that they did not access or receive in the past?

Does the initiative involve a new or significantly changed collection, use or disclosure of PHI?

YES:	NO:
PIA required. Review PIA procedures in section 6.0 above.	Proceed to Step 3 ↓

Step 3 – Determine if the initiative implements a new or significantly changed communication or IT system for PHI

Questions to consider:

What is considered to be a communication or IT system?

> Any new electronic system or platform that stores, collects or transmits PHI, some examples are a virtual care platform, electronic medical records, secure text messaging apps, dictation software or apps, etc.

Are you implementing a new system or communication technology?

Are you upgrading an existing system or communication technology?

Does the upgrade introduce significant changes to the system, such as a move from PHI being stored locally on a server to using cloud-based technology or introducing mobile access or devices?

Does the initiative involve a new or significantly changed communication or IT system for PHI?

YES:	NO:
PIA required. Review PIA procedures in section 6.0 above.	PIA not mandatory. Consider privacy review, if applicable.

Optional Step 4 (as applicable) - Determine if initiative involves data matching of PHI

Very few Health PEI initiatives involve a new data matching, which is defined as:

> the creation of individually identifying personal health information by combining individually identifying personal health information, de-identified personal health information or other information from 2 or more electronic databases or 2 or more electronic records, without the consent of the individuals to whom the information relates

Questions to consider:

Does the initiative involve PHI?

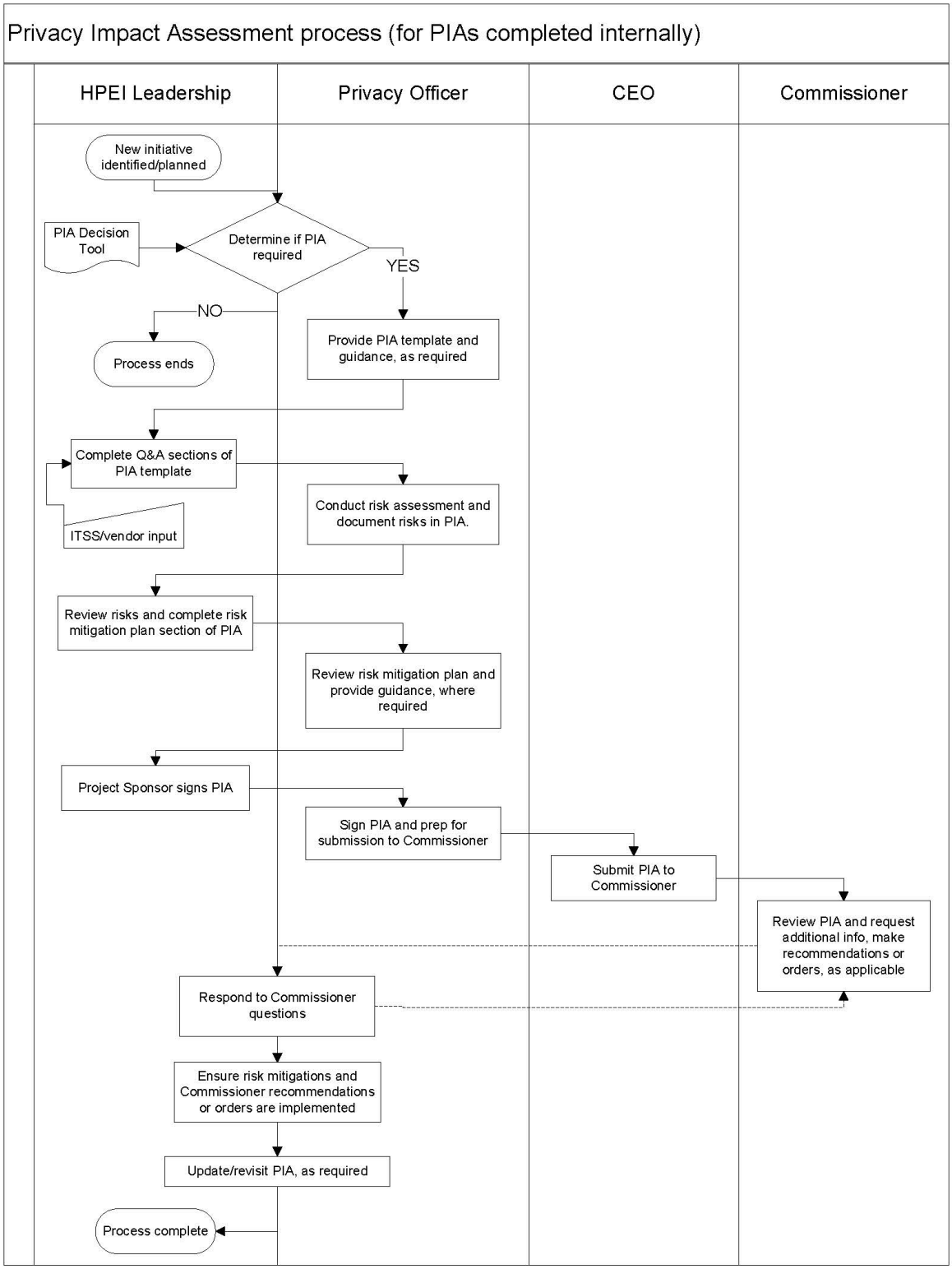
See Step 1 above.

Will the PHI be linked or combined with PHI in the custody of an external custodian (examples may include a researcher, Island EMS, private health clinic)?

Does the initiative involve data matching of PHI?

YES:	NO:
PIA required. Review PIA procedures in section 6.0 above.	PIA not mandatory. Consider privacy review, if applicable.

Appendix B – PIA Process Map



Appendix C – 10 Privacy Principles

The Canadian Standards Association (CSA) released the Model Code for the Protection of Personal Information in 1996. These 10 Privacy Principles are generally accepted as establishing a framework of privacy best practices and form the basis for the majority of health privacy legislation and policy in all jurisdictions.

1. Accountability

This principle states that an organization is responsible for personal information under its control. The organization should designate an individual or individuals to be accountable for the organization's compliance with the principles stated in the Code. An organization needs to implement policies and practices that will help them respect the principles.

2. Identifying Purposes

An organization should identify the purposes for collecting information at or before the time of collection. This will enable the organization to determine which information needs to be collected in order to meet their needs. This goes hand in hand with the Limiting Collection principle (#4). Depending on the manner in which information is collected, this principle can be fulfilled orally or in writing. For example, an application form may explain the purposes of information collection to an individual.

3. Consent

Where it is appropriate, an individual must have knowledge of and give consent to the collection, use or disclosure of personal information. An organization should make a reasonable effort to inform individuals of the purposes for collecting information. Consent should be meaningful; the purposes should be explained in such a way that the individual can reasonably understand the use and disclosure of their personal information. Individuals are entitled to withdraw consent at any time.

4. Limiting Collection

Personal information should only be collected as necessary for the purposes that the organization has identified. This includes limiting the amount and type of information. The information should be collected by fair and lawful means.

5. Limiting Use, Disclosure and Retention

An organization should not use personal information for new purposes, unless it has the consent of the individual, or as required by law. Personal data should only be retained as long as is necessary to fulfill the organization's stated purposes. An organization should develop specific guidelines and procedures governing the destruction of personal information.

6. Accuracy

In order to meet the intended purposes, personal information should be accurate, complete and up-to-date. This principle aims to minimize the possibility that incorrect information is used to make a decision about an individual. This also applies to information disclosed to third parties.

7. Safeguards

An organization should implement appropriate security safeguards to protect the personal information collected. The appropriate safeguard should be determined by the sensitivity, amount, distribution, format and method of storage of the information. Employees in the organization should be aware that confidentiality of personal information should be maintained.

8. Openness

An organization should be open about its personal information policies and practices. Individuals should be able to access an organization's policies and practices relatively easily. The method of disseminating such information depends on the nature of the organization. This may include brochures, mail to customers, online access or toll-free information lines.

9. Individual Access

Individuals should be informed of the existence, use and disclosure of their personal information. Individuals should have access to their personal information and be able to question and correct the accuracy and completeness of this information.

10. Challenging Compliance

Individuals should be able to challenge an organization's compliance with the above principles. The person accountable for an organization's compliance will be responsible for dealing with inquiries, challenges or complaints. An organization should investigate all complaints and if it is necessary, adjust its policies and practices appropriately.

Footnote https://www.cippguide.org/2010/06/29/csa-model-code/

Appendix D – Privacy Review

Privacy advice and considerations for initiatives not requiring a mandatory privacy impact assessment

Review the *Health PEI Privacy and Protection of Personal Health Information Policy* to ensure the initiative will be compliant with the policy.

Consider the guiding principles of privacy-by-design when planning the initiative, which include:

Be proactive, rather than reactive – prevent privacy incidents from occurring

Privacy by default – ensure individual PHI is protected without the individual needing to opt in or turn on privacy protective features

Privacy embedded into design – safeguards should be fully integrated into the initiative and not be added on after the fact

Full lifecycle protection – ensure PHI is safe and handled appropriately from collection to disposition

Consider physical privacy, i.e. safeguards built into the location or environment of the initiative to protect individual privacy. This can include measures to prevent others from overhearing or observing an individual's PHI.

Basic questions:

Will the initiative collect the minimum amount of PHI required to achieve the purpose?

Will PHI be used and disclosed only for the purposes of providing care or for other purposes authorized by the *Health Information Act*?

Will the PHI be retained according to the applicable retention and disposition schedule?

Are there safeguards in place (administrative, physical and technical) to adequately protect the PHI?