



PRIVACY IMPACT ASSESSMENT MANUAL

How to Complete a PIA

A high level guideline on Privacy Impact Assessments (PIA) for Yukon Government Employees

Published November 29, 2017, Version One

Developed in partnership with Elemental Privacy & Security Consulting Inc.
Info@PrivacySecurity.ca



Table of Contents

| | |
|--|----|
| Glossary of Terms..... | 3 |
| 1.0 Purpose | 8 |
| 2.0 Background | 8 |
| 2.1 What is a PIA? | 8 |
| 2.2 CSA Model Code for the Protection of Personal Information (PI) | 8 |
| 2.3 What is a Privacy Management Plan?..... | 14 |
| 2.4 What is a Security Management Plan? | 15 |
| 2.5 Why do you need to conduct a PIA? | 15 |
| 2.5.1 Policy | 15 |
| 2.5.2 Legislation | 15 |
| 2.5.3 Best Practice..... | 15 |
| 2.6 When do you need to conduct a PIA? | 16 |
| 3.0 What is Risk and how do we assess it? | 17 |
| 4.0 PIA Template Overview | 18 |
| 5.0 How to Conduct a PIA | 19 |
| 5.1 Collecting Information & Supporting Documentation | 19 |
| 5.2 Documenting the System/Project..... | 20 |
| 5.2.1 Description of the Project | 20 |
| 5.2.2 Project Scope / PIA Scope | 20 |
| 5.2.3 Parties Involved..... | 20 |
| Stakeholder | 21 |
| PHR Portal Users | 21 |
| Individuals who access their personal health information via the Personal Health Record (PHR) Portal.. | 21 |
| Provide their consent for the collection, use and disclosure of their PHI via the PHR portal, in accordance with <i>HIPMA</i> s. 33..... | 21 |
| Acme System Hosting Services | 21 |
| Health and Social Services | 21 |
| HSS is acting as custodian of the records in the PHR as defined under <i>HIPMA</i> s. 2. | 21 |
| 5.2.4 Objectives & Benefits..... | 21 |
| 5.2.5 Governance | 21 |
| 5.2.6 Contractual Obligations | 22 |
| 5.2.7 Functional Overview / Business Requirements | 22 |

| | |
|--|----|
| 5.2.8 Component Overview | 23 |
| 5.2.9 Technical Overview | 25 |
| 5.2.10 Core Business Flows (or Work Flows) | 25 |
| 5.3 Data Flows..... | 26 |
| 5.3.1 Types of Data (field level or clusters)..... | 26 |
| 5.3.2 Data Storage..... | 27 |
| 5.3.3 Data Flow Mapping..... | 27 |
| <i>*In the PIA Template refer to section 2 “Data Flow Mapping and Tables”.</i> | 27 |
| 5.3.4 Data Flow Tables | 28 |
| 5.4 Legislative Analysis..... | 30 |
| 5.4.1 HIPMA | 30 |
| 5.4.2 ATIPP | 30 |
| 5.4.3 Other | 30 |
| 5.5 Privacy Analysis | 31 |
| 5.5.1 Principle 1: Accountability | 31 |
| 5.5.2 Principle 2: Identifying Purposes..... | 32 |
| 5.5.3 Principle 3: Consent | 34 |
| 5.5.4 Principle 4: Limiting Collection..... | 35 |
| 5.5.5 Principle 5: Limiting Use, Disclosure and Retention | 35 |
| 5.5.6 Principle 6: Accuracy | 37 |
| 5.5.7 Principle 7: Safeguards..... | 38 |
| 5.5.8 Principle 8: Openness..... | 40 |
| 5.5.9 Principle 9: Individual Access | 41 |
| 5.5.10 Principle 10: Challenging Compliance..... | 42 |
| 6.0 Assessing Risk & Mitigation Strategies | 42 |
| 7.0 PIA Reviews and Approvals..... | 43 |
| 8.0 PIA Addendums..... | 43 |
| Schedule 1: Health Information Protection and Management Act (HIPMA) Summary | 45 |
| HIPMA General Regulation | 49 |
| Yukon Health Information Network (YHIN) Regulation | 51 |
| Schedule 2: Access to Information and Protection of Privacy Act (ATIPP) Summary..... | 52 |
| Schedule 3: Detailed Technical and Security Questionnaire | 56 |

Glossary of Terms

| Term | Description |
|--|--|
| Access to Information and Protection of Privacy Act (ATIPP Act) | <p>The <i>Access to Information and Protection of Privacy Act</i> came into force on July 1, 1996.</p> <p>The purposes of the <i>ATIPP Act</i> are to make public bodies more accountable to the public and to protect personal privacy. The Act does this by giving the public a right of access to records, subject only to limited and specific exceptions; giving individuals a right of access to, and a right to request correction of, their own personal information; and preventing the unauthorized collection, use or disclosure of personal information by public bodies.¹</p> |
| Agent (from HIPMA) | <p>“agent” of a custodian means a person (other than a person who is prescribed not to be an agent of the custodian) who acts for or on behalf of the custodian in respect of personal health information, including for greater certainty such a person who is</p> <ul style="list-style-type: none"> (a) an employee of the custodian, (b) a person who performs a service for the custodian under a contract or agency relationship with the custodian, (c) an appointee, volunteer or student, (d) an insurer or liability protection provider, (e) an information manager, (f) if the custodian is a corporation, an officer or director of the corporation, or (g) a prescribed person. |
| Collection (of PHI) (from HIPMA) | Means to gather, acquire, receive or obtain by any means from any source, but does not include the transmission of information between a custodian and an agent of that custodian. |
| Collection (of PI) (from ATIPP act) | <p>The term “collection” is not specifically defined in the <i>ATIPP act</i>. Section 29 sets out the following basic requirement:</p> <p>No personal information may be collected by or for a public body unless</p> <ul style="list-style-type: none"> (a) the collection of that information is authorized by an Act of Parliament or of the Legislature; (b) that information is collected for the purposes of law enforcement; or (c) that information relates to and is necessary for carrying out a program or activity of the public body. |

¹ <http://www.ombudsman.yk.ca/yukon-information-and-privacy-commissioner/for-public-bodies/atipp-act>

| Term | Description |
|--|--|
| Control (of data) | The accountability for information, even when the information leaves the organization's direct custody. ² |
| Consent | <p><i>HIPMA</i>, when the context permits, includes the power to give, refuse and withdraw consent for the collection, use and disclosure of PHI. Under the act, consent may be implied, unless the act specifies express consent is required. To be valid, consent must:</p> <ul style="list-style-type: none"> a) be knowledgeable³; b) relate to the personal health information; and c) be given voluntarily and not obtained by fraud or misrepresentation. |
| CSA Model Code for the Protection of Personal Information | The Canadian Standards Association's (CSA) Model Code for the Protection of Personal Information (PI) is the foundation for Canadian privacy legislation including <i>HIPMA</i> . |
| Custodian (from <i>HIPMA</i>⁴) | <p>"custodian" means a person (other than a person who is prescribed not to be a custodian) who is:</p> <ul style="list-style-type: none"> (a) the Department, (b) the operator of a hospital or health facility, (c) a health care provider, (d) a prescribed branch, operation or program of a Yukon First Nation, (e) the Minister, (f) a person who, in another province <ul style="list-style-type: none"> (i) performs functions substantially similar to the functions performed by a health care provider, and (ii) is, in the performance of those functions, subject to an enactment, of Canada or a province, that governs the collection, use and disclosure of personal information or personal health information, or (g) a prescribed person. |

² Adapted from the COACH Guidelines 2011

³ *HIPMA* S.39 An individual's consent to the collection, use or disclosure of their personal health information is knowledgeable only if the individual knows: (a) the purpose of the collection, use or disclosure of the personal health information; (b) that they may give or withhold consent and having once given consent, may withdraw that consent; and (c) that without their consent the personal health information can be collected, used or disclosed only in accordance with the provisions of this Act and the regulations. S.Y. 2013, c.16, s.39

⁴ The *ATIPP* act uses the *HIPMA* definition for custodian.

| Term | Description |
|---|--|
| Custody (of data) | The organization that has the information systems that house the data within its possession, and having the responsibility for the day-to-day operation, management and security of those information systems. |
| Disclosure (of PHI) (from <i>HIPMA</i>) | “disclose”, in relation to information in the custody or control of a person, means making the information available or releasing it to another person, but does not include either using the information or its transmission between a custodian and an agent of that custodian. |
| Disclosure (of PI) (from <i>ATIPP</i> act) | “disclosure”, is not specifically defined in the <i>ATIPP</i> act, but the permitted conditions and requirements for disclosure are dealt with extensively in Part 2 and Part 3. |
| GAM | General Administration Manual (Yukon government) |
| Health Information Privacy and Management Act (<i>HIPMA</i>) | The <i>Health Information Privacy and Management Act (HIPMA)</i> is a new, modern, comprehensive law similar to privacy laws in most Canadian provinces and territories. <i>HIPMA</i> balances protection of personal health information with the information needs of Yukon health care workers so that they can provide the best care possible. Among many things, <i>HIPMA</i> sets out how personal health information must be protected, an individual’s right to have access to their personal health record, and when and how personal information can be collected, used and disclosed. ⁵ |
| HSS | Yukon Government Department of Health and Social Services |
| IPC | Information and Privacy Commissioner |
| IT | Information Technology |
| Personal Health Information (PHI) (from <i>HIPMA</i>) | <i>HIPMA</i> defines “personal health information” of an individual to mean the: (a) health information of the individual, and (b) except as prescribed, prescribed registration information and prescribed provider registry information in respect of the individual. |

⁵ adapted from http://www.hss.gov.yk.ca/pdf/hipmadiscussion_en.pdf

| Term | Description |
|--|---|
| Personal Information (PI) | <p><i>HIPMA</i> and <i>ATIPP</i> both define “personal information” to mean recorded information about an identifiable individual, including</p> <ul style="list-style-type: none"> (a) the individual’s name, address, or telephone number, (b) the individual’s race, national or ethnic origin, colour, 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 care history, including 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, and (i) the individual’s personal views or opinions, except if they are about someone else. |
| PI/PHI | Personal information / personal health information |
| Privacy Impact Assessment (PIA) | A standard risk assessment tool used to identify and mitigate potential privacy risks of new or redesigned systems, programs, services, or legislation. |
| Public Body (from <i>ATIPP</i> act) | <p>“public body” means:</p> <ul style="list-style-type: none"> (a) each department, secretariat or other similar executive agency of the Government of Yukon, and (b) each body designated as a public body in a regulation made under section 68, <p>but for greater certainty does not include:</p> <ul style="list-style-type: none"> (c) the Legislative Assembly Office or offices of the members of the Legislative Assembly, (d) the chief electoral officer and election officers acting under the Elections Act, or (e) a court established by an enactment. |
| Security Threat Risk Assessment (STRA) | An assessment that identifies various threats to Information Technology (IT) systems, determines the level of risk these systems are exposed to, and recommends appropriate levels of protection. |

| Term | Description |
|--|--|
| Use (of PHI) (from HIPMA) | <p>“use” in relation to personal health information in the custody or control of a person includes handling or dealing with the personal health information in any manner whatsoever, other than by collecting or disclosing it.</p> <p>Under <i>HIPMA</i>, “use” can also mean the transmission of the personal health information between a custodian and an agent of that custodian.</p> |
| Use (of PI) (from ATIPP act) | <p>“use” is not specifically defined in the <i>ATIPP</i>, but the requirements are set out in section 35(1): A public body may use personal information only:</p> <ul style="list-style-type: none"> (a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose; (b) if the individual the information is about has consented to the use; or (c) for the purpose for which that information may be disclosed to that public body under sections 36 to 39. |
| YHC | Yukon Hospital Corporation |
| YHCIP Card | <p>The certificate of registration or identity card issued to an insured person for the purposes of the <i>Health Care Insurance Plan Act</i>.</p> <p>Note that the YHCIP number is considered “health information” under paragraph (b) of the definition in <i>HIPMA</i> subsection 2(1).</p> |
| Yukon Health Information Network (YHIN) | <p>From <i>HIPMA</i> subsection 2(1): “Yukon health information network” means the electronic health information network, if any, designated under section 72, and includes any component or system of such a network.</p> |

1.0 Purpose

The purpose of this manual is to serve as a guideline for Yukon Government (YG) employees on how to complete a Privacy Impact Assessment (PIA). In addition to step-by-step instructions on conducting a PIA using the standard template, there are descriptions of the type of information required, possible sources of that information, questions to ask and expected potential answers, including those answers that may trigger a risk.

Information related to foundational concepts such as consent, as well as the development of work flows, data flows, and legislative considerations described in the manual will assist in developing YG employees' expertise to enable them to conduct most PIAs in-house.

2.0 Background

2.1 What is a PIA?

A PIA is a standard risk management tool used to identify and mitigate potential privacy risks that may be introduced by new or redesigned systems, programs, services, or legislation. A PIA helps to confirm that legal authorities exist for the collection, use, retention and disclosure of personal information involved in an initiative and demonstrates an organization's commitment to due diligence to protect personal information in its custody or control. PIAs can promote a culture of privacy within an organization, as well as improve operational efficiencies and reduce organizational risk by minimizing excessive collection, use, retention and disclosure of personal information.

The tool is based upon the Canadian Standards Association's (CSA) Model Code for the Protection of Personal Information (PI) which is also the foundation for Canadian privacy laws and privacy "best practices".

2.2 CSA Model Code for the Protection of Personal Information (PI)

CSA's Model Code for the Protection of Personal Information (CAN/CSA-Q80-96) is summarized below⁶.

Principle 1. Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

- Accountability for the organization's compliance with the principles rests with the organization's designated individual(s) (such as a Privacy Officer), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).
- The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.
- An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use

⁶ From the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, Schedule 1.

URL: <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-11.html#h-26>

contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

- Organizations shall implement policies and practices to give effect to the principles, including:
 - implementing procedures to protect personal information;
 - establishing procedures to receive and respond to complaints and inquiries;
 - training staff and communicating to staff information about the organization's policies and practices; and
 - developing communication materials to explain the organization's policies and procedures in the event that an inquiry is received.

Principle 2. Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

- The organization shall document the purposes for which personal information is collected in order to comply with Principle 8: Openness and Principle 9: Individual Access.
- Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. Principle 4: Limiting Collection requires an organization to collect only that information necessary for the purposes that have been identified.
- The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.
- When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to Principle 3: Consent.
- Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.
- This principle is linked closely to the Principle 4: Limiting Collection and Principle 5: Limiting Use, Disclosure, and Retention.

Principle 3. Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except when inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list

from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

- Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).
- The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.
- An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.
- The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.
- In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.
- The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).
- Individuals can give consent in many ways. For example:
 - an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
 - a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

- consent may be given orally when information is collected over the telephone; or
- consent may be given at the time that individuals use a product or service.

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

Principle 4. Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

- Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle.
- The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.
- This principle is linked closely to the Identifying Purposes principle and the Consent principle.

Principle 5. Limiting Use, Disclosure and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

- Organizations using personal information for a new purpose shall document the rationale for why the information is absolutely necessary to achieve the new purpose.
- Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.
- Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.
- This principle is closely linked to the Consent principle, the Identifying Purposes principle, and the Individual Access principle.

Principle 6. Accuracy

Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

- The extent to which personal information shall be accurate, complete, and up-to-date will depend upon accuracy of the information at the time of collection, and the use of the information, taking into account the interests of the individual. Information shall be sufficiently

accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

- An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.⁷
- Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

Principle 7. Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

- The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.
- The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, as well as the amount, distribution, format of the information, and the method of storage. Information that is more sensitive should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Principle 3 - Consent.
- The methods of protection should include
 - physical measures, for example, locked filing cabinets and restricted access to offices;
 - organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and
 - technological measures, for example, the use of passwords and encryption.
- Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.
- Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

Principle 8. Openness

An organization shall make readily available to individuals’ specific information about its policies and practices relating to the management of personal information.

- Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.
- The information made available shall include
 - the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;

⁷ An update to PI would be a further “collection” which should only happen if required for the business process. For example, a Community Health Centre treats a visitor to the Territory and refers the patient to Whitehorse General Hospital. There may be no clinical purpose for the Health Centre collecting additional PHI related to the patient’s acute care treatment (such as a discharge summary from the hospital) if it is unlikely that the patient will ever return to the Health Centre.

- the means of gaining access to personal information held by the organization;
- a description of the type of personal information held by the organization, including a general account of its use;
- a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
- what personal information is made available to related organizations (e.g., subsidiaries).
- An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

Principle 9. Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

- Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.
- An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.
- In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.
- An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.
- When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition

of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

- When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

Principle 10. Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

- The individual accountable for an organization's compliance is discussed in Principle 1 - Accountability.
- Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.
- Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.
- An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

2.3 What is a Privacy Management Plan?

A Privacy Management Plan is an assessment tool designed to help ensure privacy controls such as the designation of a privacy officer, a personal information inventory, use of risk assessment tools including PIAs, Information Sharing Agreements (ISA), and employee training on privacy are in place and adequate.

Privacy Management Plan⁸

What is the purpose of completing a privacy management plan?

A Privacy Management Plan is a privacy risk assessment tool that can be utilized by program managers to proactively measure whether the privacy controls included in General Administration Manual (GAM) 2.27 – Privacy Management Policy are in place. Privacy controls can serve to reduce risks associated with the collection, use or disclosure of personal information, including reducing the risk of a privacy breach.

Is completing a privacy management plan required?

No, completing a privacy management plan is not a requirement under GAM 2.27 – Privacy Management Policy or its supporting policies.

⁸ From *Privacy Management Plan – Guidance*, Highways and Public Works, Yukon government.

Who should complete a privacy management plan?

It is recommended program managers or designates complete a privacy management plan for the program or activity they are responsible for.

When should I complete a privacy management plan?

A privacy management plan can be completed anytime as it is a proactive tool to assist program managers or designates to conduct a privacy risk assessment on their programs.

Which of the controls included in the privacy management plan should I prioritize?

Because program managers face resource constraints, program managers may not be able to implement all of the controls listed in the privacy management plan at once.⁹¹⁰

2.4 What is a Security Management Plan?

A Security Management Plan addresses physical, technical and administrative safeguards to protect the confidentiality, integrity and availability of information and may include Security Threat Risk Assessments (STRA) as part of its ongoing plan. A Security Threat Risk Assessment (STRA) is a separate assessment that identifies various threats to IT systems, determines the level of risk these systems are exposed to, and recommends appropriate levels of protection. If adding new applications or systems to an IT environment, making modifications to an existing environment, or sharing information with new external entities, then a STRA on the new components will help ensure no new risks are introduced.

2.5 Why do you need to conduct a PIA?

2.5.1 Policy

Conducting a PIA is mandatory under the Government of Yukon *PIA Operational Policy*.

2.5.2 Legislation

PIAs are required for Health and Social Services Department (HSS) and the Yukon Hospital Corporation (YHC) under the Health Information Protection and Management Act (*HIPMA*) general regulation:

15(2) A custodian... must conduct a privacy impact assessment before it (a) implements any measure that, in the opinion of the Minister, is a significant change to an existing information system used to process personal health information; or (b) commences the operation of a new information system intended to be used to process personal health information.

2.5.3 Best Practice

Conducting a PIA can show “due diligence” has been done by the organization/department that will be collecting personal information, provided the PIA is completed in a full and comprehensive manner. This simply means that the organization can demonstrate through the PIA that appropriate measures have been put in place to protect the confidentiality of the personal information it has in its custody and/or control.

⁹ From *Privacy Management Plan – Guidance*, Highways and Public Works, Yukon government

¹⁰ Program managers should consider the level of risk associated with the collection, use and disclosure of PHI and the resources required to implement the controls to mitigate the risk, as well as reduce the potential of a breach.

2.6 When do you need to conduct a PIA?

Under the Yukon Government PIA Operational Policy, PIAs are mandatory for all proposed or amended IT systems, programs, services or legislation.

HIPMA mandates a PIA be conducted before implementing any significant change to an existing information system used to process PHI or commencing the operation of a new information system intended to be used to process PHI. This is true even if a PIA was conducted on the original system. Further, the PIA must be submitted to the Yukon Information and Privacy Commissioner (IPC) prior to the change being implemented or the new system activated. While a project may proceed once the PIA has been submitted to the IPC, it is strongly recommended that your project work plan allow for ample time to submit and respond to any feedback received from the IPC prior to implementation.

Based on the IPC's *Guidance for Public Bodies on Accountable Privacy Management (available online)*, at minimum, a public body should complete a PIA for all new projects involving personal information, such as the development of an electronic system that will process personal information and for any new collection, use or disclosure of personal information. PIAs should also be conducted for significant modifications of existing systems, programs or activities.




Questions to ask:

- Are you designing a new program, service or activity, making significant changes to an existing program or service, or converting from a conventional service delivery mode to an electronic one?
- Does the program require you to collect, use or disclose any personal information, such as name, address, age, identifying number, educational, medical or employment history, etc.?
- Will the program require that you collect, use or disclose more personal information or more sensitive personal information than in the past?
- Are you shifting from collecting personal information directly from the individual to indirect collection of personal information?
- Are you shifting from collection with express consent of the individual to without consent?
- Will it be necessary to develop mechanisms to notify individuals about their privacy rights or to obtain the consent of individuals to collect, use and/or disclose their personal information?
- Will the program require you to collect personal information from other Yukon Government programs, institutions, health information custodians, other governments, or the private sector?
- Is the operation of a program, service or IT system shifting to third party service providers?
- Will the personal information generated by the program be used in decision-making processes that directly affect individuals, such as program/service eligibility or enforcement activities?
- Will the personal information generated by the program be used for any other purposes, including research and statistical purposes?
- Will the personal information be shared with any other organizations for any purposes other than for which it was originally collected?
- Are you introducing new client identifiers?
- Do you anticipate that the public will have any privacy concerns with the proposed initiative?

- Are you introducing changes to the business systems or infrastructure architecture that affect the physical or logical separation of personal information or the security mechanisms used to manage and control access to personal information?

If the answer is “Yes” to any of the above questions, you will need to conduct a PIA.

| | |
|---|---|
|  | <p>Remember:</p> <p>It is strongly recommended that you allow ample time in your project work plan if a PIA is required to be submitted to the IPC. Doing so demonstrates your commitment to due diligence as it will allow you to receive and action any feedback received prior to implementation.</p> |
|---|---|

3.0 What is Risk and how do we assess it?

The Yukon Government defines “risk” as the effect of uncertainty on objectives¹¹.

- An *effect* is a deviation from the expected - positive and/or negative
- *Uncertainty* is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence or likelihood.
- *Objectives* can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project product and process)

Risk is assessed from a “business” perspective. Risk is sometimes difficult to measure and quantify because organizations have different tolerances for risk. Similar situations therefore may result in different conclusions about what the risk means to the organization or the individuals whose personal information is involved.

For example, at an individual level, one person will decide that parachuting is too risky to try while another person will “jump” at the chance. The same is true with organizations and the employees who assess the privacy risks identified through the PIA exercise.

Once identified, the challenge of measuring risk can be addressed based on two factors:

1. The *likelihood* of an incident occurring:

HIGH: There is a very good chance that the risk to privacy will occur, particularly if there is a history of it having frequently occurred in this or similar environments.

MEDIUM: There is a good chance that the risk to privacy will occur, particularly if there is a history of it having previously occurred in this or similar environments.

LOW: It is very unlikely that this risk to Privacy will occur.

2. The *impact* of the incident should it occur. You should consider the impact on the organization as well as impact on the individuals who are the subject of the personal information:

HIGH: There would be very serious – exceptionally grave consequences if the risk were to occur.

¹¹ HSS Corporate Policies; Risk Management Policy; GOV-002; Dec 1, 2010

MEDIUM: There would be significant consequences if the risk were to occur.

LOW: There would be low - marginal consequences if the risk were to occur.

| Impact | Risk Reference Table | | |
|------------|----------------------|--------|-----------|
| High | Medium | High | Very High |
| Medium | Low | Medium | High |
| Low | Very Low | Low | Medium |
| Likelihood | Low | Medium | High |

In the table above, the intersection of “Impact” and “Likelihood” gives a rating for the risk.

PIAs use a “Risk Table” to record risks, ratings, mitigation recommendations and accountability. The Risk Table can look like this:

| # | Privacy Risk / Threat | Likelihood | Impact | Risk Level | Mitigation Strategy | Accountability | Risk Level After Mitigation |
|---|---|------------|--------|------------|---|-----------------------------------|-----------------------------|
| 1 | Records of PI are stored in a shoebox under the desk, creating a risk that PHI can be accessed by unauthorized individuals. | L | M | L | Move the records of PI to a filing cabinet that is securely locked when not in use. | Manager - Records Management Unit | VL |

No matter what the initiative is, there will always be risk. It is through the PIA process that risks are identified, mitigation strategies identified and the position of the individual to whom accountability is assigned. As the PIA drafter you will have a good perspective on the level of risk by virtue of having conducted the analysis, however be prepared to be challenged on your wording, number of risks identified and your ratings, and remember that the business owners should have the final say in regards to the risk ratings.

In the approval process, one or more individuals will “sign off” on the PIA indicating acceptance of the risks in the context of the mitigation strategies.

4.0 PIA Template Overview

PIA templates vary from simplistic to very complex. For all Yukon government departments listed in GAM 2.1 the template to be used is mandated in the PIA Operational Policy which states:

“PIAs must be completed in the template developed by the ATIPP office, unless otherwise approved by the director of Corporate Information Management.”

Section 5.0 *How to Conduct a PIA* provides details on the various components you may encounter in any given PIA template and guidance on how to complete them.



Remember:

Always be sure that you obtain the most current version of the template before beginning the assessment.

5.0 How to Conduct a PIA

Regardless of how simple or complex your initiative is, how you conduct a PIA remains consistent. Collecting specific information about the project, identifying the key players and stakeholders, along with the type of, and manner in which, personal information will be collected, used, retained, disclosed, secured or disposed of are all part of the PIA process. This section breaks the process down into simple steps and provides you with example questions to walk you through conducting a PIA regardless of the template being used. A detailed set of questions are provided in the form of a “Privacy Questionnaire” in Schedule 3.

5.1 Collecting Information & Supporting Documentation

**In the PIA Template refer to section 0.1 “Policies, Forms and Reports”*

You are not alone when conducting a PIA. Prior to conducting a PIA, identifying other individuals who have knowledge of the initiative, the business area and processes is critical. A PIA also requires the expertise of others such as information technology and security analysts, and your *ATIPP* staff to ensure that the assessment is accurate and comprehensive.

Completing a PIA requires a lot of information, so before you begin writing be sure to gather as much information and supporting documentation as possible such as:

- Project charters;
- Business requirements;
- Forms used by the program to collect PI;
- Other applicable legislation (beyond *ATIPP* and *HIPMA*) that may be relevant;
- Operational procedures and business process documentation;
- User, administrative and/or technical manuals from vendors;
- Agreements – e.g. Services, System Access, Information Sharing, Acceptable Use;
- System documentation such as network and system architecture diagrams, data models, technical and security requirements, and system configuration;
- Policies and Procedures; and
- Previously conducted related PIAs.



Remember: Knowledge is power – the more information you know, the better your ability to conduct a thorough and accurate PIA.

5.2 Documenting the System/Project

As noted in 5.1 above, before you begin writing a PIA, be sure to gather as much information and supporting documentation as possible. This will help avoid erroneous information and repeated re-writes to the document.

5.2.1 Description of the Project

**In the PIA Template refer to section 1.1.1 “Description of the Project”*

This section of the PIA should provide a general description of the project and the context in which it functions. Depending on the complexity of the initiative this may be quite lengthy and may include a Background, Current State and Future State description. For smaller initiatives a few paragraphs may suffice. Whatever the case, you want to make the reader understand why the initiative is being done and what will be accomplished in terms of functionality such as business process or patient services benefits.

5.2.2 Project Scope / PIA Scope

**In the PIA Template refer to section 1.1.2 “Scope of PIA”*

Identifying the project scope for a PIA involves documenting the specific goals, deliverables, features, functions, and deadlines. For example: *The project scope includes the installation of Software A in the XX department for use by 2 authorized staff to conduct specialized patient testing for a 3-month pilot project commencing on Jan 1, 2018 and ending on Mar 31, 2018.* This information can often be found in a Briefing Note or Project Charter for larger projects. In some cases, identifying what is out of scope can add clarity to what precisely is in scope.

The PIA scope must be clearly documented to avoid “scope creep”, which can ultimately delay obtaining approval. If your assessment is only for a three-month pilot with limited functionality and users of a new software application, be sure to make that clear in the PIA. For larger projects there may be multiple PIAs done for different stages of the project, for example conceptual, logical and physical, so it is important to clearly document exactly what the PIA scope is.

The scope may also include details regarding how updates to the PIA will be done. A PIA is a living document so it is important to identify the process for any changes to the information documented in the assessment. For example, in the case of a pilot project example noted, the scope may also state something such as “Upon completion of the pilot evaluation by May 30, 2018, a decision regarding whether the application will be decommissioned, pilot extended or usage expanded to a full implementation at XX department will be documented in an Addendum to this PIA.”

5.2.3 Parties Involved

**In the PIA Template refer to section 1.1.3 “Parties Involved”*

All parties that may collect, use, or disclose information involved in the initiative being assessed must be identified, along with the justification (purpose) and legal authority for doing so. Parties may include a vendor that may access and/or use personal information to provide support, patients that provide their information, and staff of the department/organization that collect and use the information. Business areas involved in the project should be noted in the PIA by identifying job functions and the legal authority under which they participate. Staff changes occur regularly, so apart from identifying project sponsors and signatories by name in the PIA, avoid putting individual names and instead refer to their

functions or roles. This will help avoid unnecessary updates to the assessment when staff change roles. Remember to consider other external organizations or individuals that may have a role in an initiative such as a vendor that may be providing support.

Example:

| Stakeholder | Function | Legal Authority |
|-------------------------------------|---|--|
| PHR Portal Users | Individuals who access their personal health information via the Personal Health Record (PHR) Portal. | Provide their consent for the collection, use and disclosure of their PHI via the PHR portal, in accordance with <i>HIPMA</i> s. 33. |
| Acme System Hosting Services | Acme provides a number of services to Health and Social Services in support of the Personal Health Record web site solution including: <ul style="list-style-type: none"> • Server, application and database hosting • Transaction logging • Custody of the PHR portal PHI • Tier 2 application support | Acme is acting as an information manager under <i>HIPMA</i> s. 51. |
| Health and Social Services | HSS is responsible for: <ul style="list-style-type: none"> • PHR solution design, development, maintenance and enhancement • Business / technical requirements to Acme for the provision of hosting and other services • Developing communications materials for the public • Developing and delivering training for HSS staff • Tier 1 Service Desk support | HSS is acting as custodian of the records in the PHR as defined under <i>HIPMA</i> s. 2. |

In addition to the above type of summary of project participants, specific functional details will be included in the data flow mapping (see sections 5.5.3: Consent and 5.5.4: Limiting Collection)

5.2.4 Objectives & Benefits

**In the PIA Template refer to section 1.1.4 "Objectives and Benefits"*

State the project's objective succinctly, as well as the anticipated benefits to the organization (i.e. time and costs efficiencies, etc.). Again, for larger projects this information is often available in existing Project Charters, Briefing Notes and other project documents.

5.2.5 Governance

Identify the relevant privacy and security organizational policies, as well as applicable laws that govern the collection, use, disclosure, retention and disposal of personal information in the PIA. As well, confirming organizational governance for the initiative will be required to identify who will review

and/or sign off on the PIA and ultimately be responsible and accountable for the project and the personal information involved. As noted earlier in this manual, the Government of Yukon *PIA Operational Policy* requires all PIAs be submitted to the *ATIPP* office for review and comment within a reasonable time frame prior to launch, and must be signed as per Policy 2.27 by the department's Deputy Minister or designate in order to be considered complete.

Remember to consider the governance structure for the project phase, as well as the structure for ongoing operations. There should be a procedure in place that allows for effective communication and decision-making among the stakeholders of the project in order to address any privacy and security issues that may arise.

5.2.6 Contractual Obligations

**In the PIA Template refer to section 3.7.9 / consult with your department's Procurement Advisor and/or Contract Coordinator*

If the initiative involves third party participants, contracts, privacy schedules and information sharing agreements (ISA) may be necessary and should be reviewed in the risk assessment. You don't need to review "business sensitive" information such as financial terms, but you will be interested in what the agreements say related to privacy and security matters. Sometimes, agreements will have a separate "Privacy Schedule", but regardless you will be looking for language that addresses requirements and obligations such as:

- Privacy training for third party staff;
- Acknowledgement of legal authority (such as a being designated as an "information manager" under *HIPMA*);
- Commitment to confidentiality;
- Notification requirement in the event of a privacy breach;
- Notification requirement prior to accessing production data containing personal information.

Others assisting you may provide this part of the assessment.

5.2.7 Functional Overview / Business Requirements

**This section is not identified in the current PIA Template – include this section in your PIA as appropriate*

Some PIA templates will include a functional overview section that describes the business requirements of a new system or service. These can be listed as in the table below. The purpose for including these in the PIA is that it establishes a "stake in the ground" for what the PIA has assessed. Particularly for PIA's done early in new project, the specific functions performed by a system may evolve based on limitations of available software, budget constraints, changes in project scope, or a phased approach to project implementation. By documenting the business requirements on which the PIA was based, you will be able to more effectively address changes that come along as the project evolves.

Example: An in-Ambulance incident management system (Paramedic Information Exchange - “PIX”)

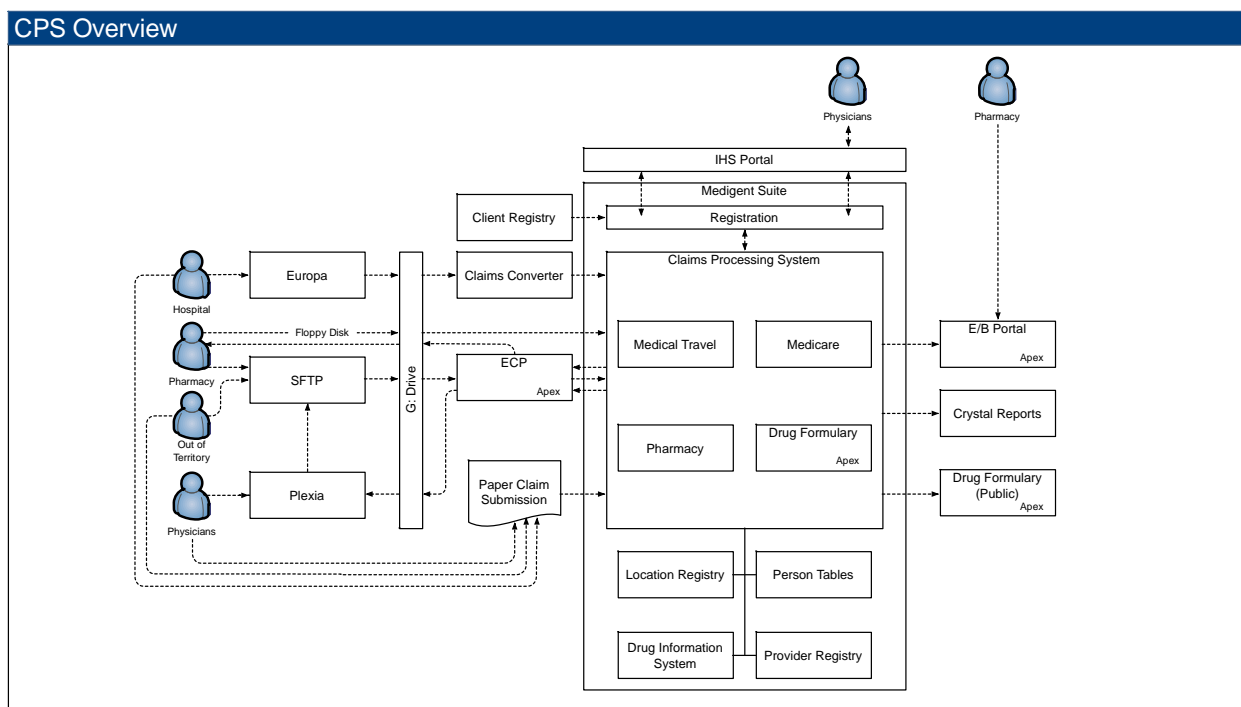
| Requirement | Comments |
|---|----------------------------------|
| 1 PIX solution must display incident information (textual incident details and map) for unit(s) assigned to the incident | Location may identify individual |
| 2 PIX solution must display following textual incident details <ul style="list-style-type: none"> Incident/Pickup Address Building Access Info like Buzzer#, entrance direction etc. Caution Notes / Hazards Incident Priority (Color coded) Chief Complaint / Problem Nature Remarks (to indicate if second unit is needed or assigned to incident, etc. Allied Agencies/Resources responding (e.g. Police/Fire etc) | Data includes PHI |
| 3 PIX solution must display a map which should provide the following information <ul style="list-style-type: none"> Incident/Pickup location and Unit's current location, etc. | |
| 4 PIX solution should allow user to provide following info updates back to central dispatch for the assigned incident: <ul style="list-style-type: none"> Patient Name(s) Patient Contact CTAS (health score) Patient Transport CTAS | Includes PHI |

5.2.8 Component Overview

**This section is not identified in the current PIA Template – include this section as required*

For PIA templates with a component overview, a description of the different pieces involved in the initiative is documented. With the cooperation of the appropriate component expert, the component overview is meant to clearly identify all of the pieces involved in the initiative to ensure that each is assessed for risk. For example, the Department of HSS uses a Claims Processing System application that is integrated with various other systems that provide file processing, reporting and viewer capabilities. These components all work together to support the range of business processes that are involved in claims processing.

Example: Claims Processing System component overview. In this case, the shaded boxes indicate out-of-scope components.



Add a table to provide a text description of each component, like this example:

| Component | Description |
|---------------------------------------|--|
| Medigent | <p>The Medigent suite includes the following modules:</p> <ul style="list-style-type: none"> • Registration • Location Registry • Person Tables • Drug Information System • Provider Registry • Medical Travel |
| Claims Processing System (CPS) | Part of the Medigent suite of services, CPS includes claims adjudication and payment processing functionality. |
| Claims Converter | Claims Converter is primarily used for importing electronically submitted claims from Yukon Hospital Corporation, and the province of Alberta into CPS. |



Remember: You are not alone -- engage the appropriate expert for each component of the initiative being assessed.

5.2.9 Technical Overview

**This section is not identified in the current PIA Template – include this section as required*

Questions related to data storage, technical environments, network security, and end user access controls would be included in the technical overview. Depending on the initiative, a technical overview can be very simple or extremely complex, and may include referencing an STRA. Remember to rely on the expertise within your department or organization to assist you with this. Vendors may also be able assist by providing relevant information. Be sure to ask for any documented processes and network diagrams that may provide further clarity to your risk assessment.

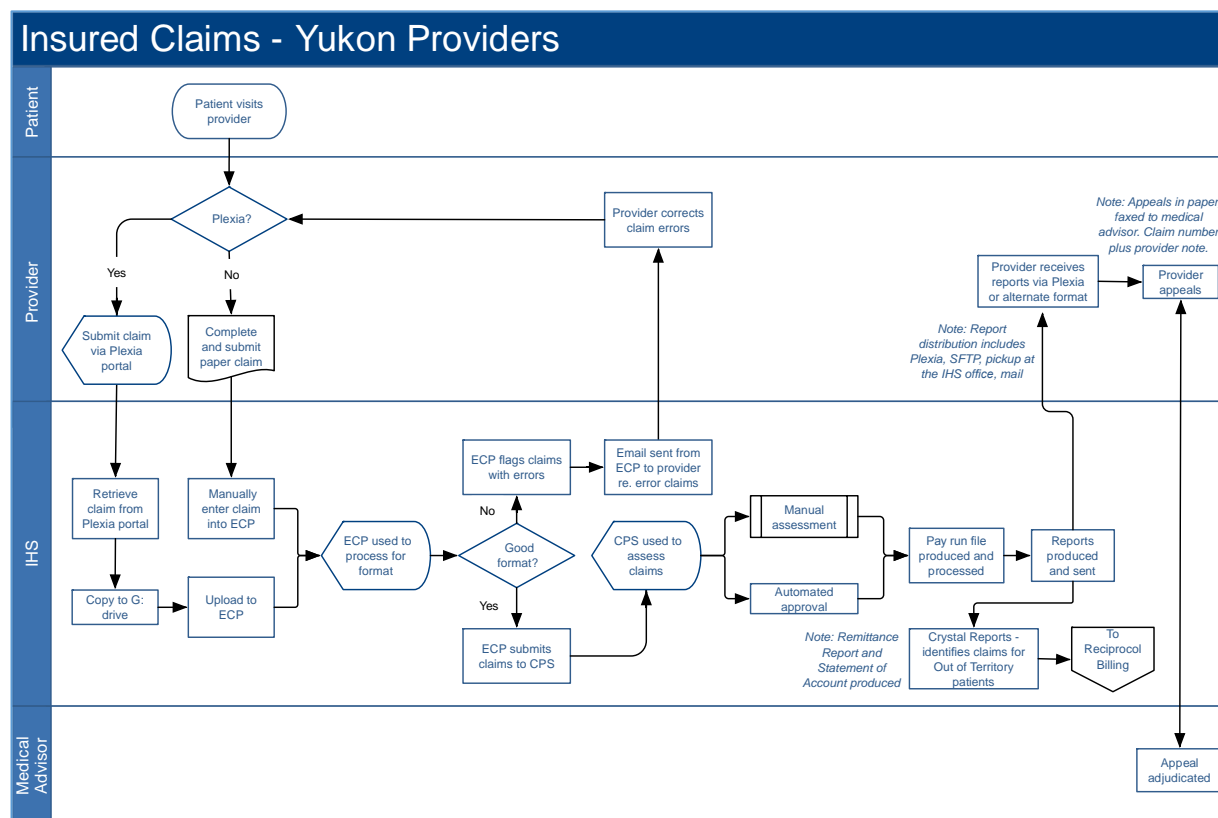
5.2.10 Core Business Flows (or Work Flows)

**In the PIA Template refer to section 2 “Data Flow Mapping and Tables” and below section 5.3*

When conducting a PIA, it is critical to understand the business/work flows involved, as well as identifying the roles of staff that will be accessing the personal information, for what purpose, when and how. Identifying the subject matter experts needed to complete business flows is critical to conducting an accurate risk assessment. This information is essential to determine if the collection, use and sharing of the information is compliant with legislation and provides the opportunity to identify inefficiencies in current processes that may be enhanced as part of the initiative. Keep a critical eye out for business processes such as duplicates of records being retained by multiple parties in a variety of formats, as these will impact the risk to privacy and may need to be addressed in the PIA.

Business process maps can take a variety of forms, but typically use “swim lanes” that isolate the steps according to the organization responsible. Table 5.2.11 on the following page is an example of a swim lane diagram:

Table 5.2.11



Remember: A business process map is critical to completing a PIA, so engage the appropriate business experts early!

5.3 Data Flows

5.3.1 Types of Data (field level or clusters)

**In the PIA Template refer to section 1.1.5 "Description of Personal Information Collected"*

It is critical to know the types of data involved in an initiative in order to assess the risk. Typically, a list of personally identifiable field level data elements, such as name, date of birth, and social insurance number is provided along with a broader description of other data clusters such as health or education history in an Appendix to the PIA. Again, depending on the complexity of each initiative the personal information involved, an Appendix may not be necessary, or you may have multiple Appendices.

The types of data and/or data clusters (such as demographic data) involved must be identified to help determine the security safeguards that should be implemented, as well as to determine the level of risk associated with an initiative. When completing this section of the PIA always consider if the collection, use and disclosure of PI/PHI involved in the initiative is the least amount necessary to meet the specified purpose. Sensitivity of the data should also be considered when determining the security controls needed

and will also impact the risk level. For example, a person's name, while personal information, is not as sensitive as their results from a blood test related to cancer diagnosis.

When conducting this section of a PIA keep alert for terms such as "we'd like to have this information", "we might need the information", "it would be nice to have this in case we need it in future" as these should raise a red flag and you should ask more questions to confirm there is a legitimate need that is authorized under legislation for the data.

5.3.2 Data Storage

**In the PIA Template refer to section 3.7.6 "Where and How Information is Stored"*

Identifying where the data will be stored, along with its retention and disposal schedule, is important to ensure information is only retained for the period of time legally permitted and then disposed of in an appropriate manner depending on the type of data involved and your organization's standards. As well, it is critical to document where the data is stored in order to ensure a thorough risk analysis. For example, data stored on an unencrypted USB is at far more risk than data stored on the organization's secure network in a restricted folder. For electronic data storage, your Information Technology staff should be able to provide you with the information needed. Stay alert for any references about duplicate records being retained in various formats as this may impact the risk assessment.

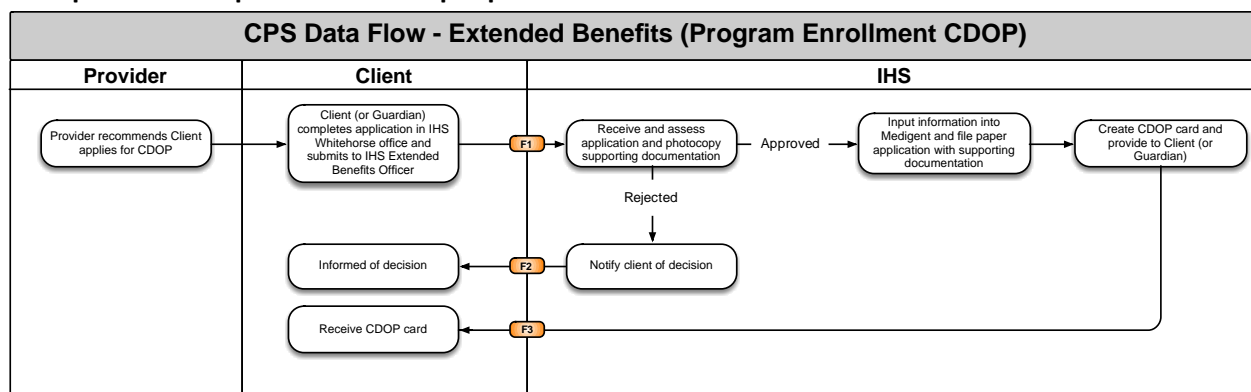
5.3.3 Data Flow Mapping

**In the PIA Template refer to section 2 "Data Flow Mapping and Tables"*

Data flows are probably the most critical part of the PIA as they identify what information is going where, when, to whom, and how. This task involves mapping all the flows of personal information within the scope of the project. Consider all formats (i.e. paper and electronic) from creation or collection until final disposition (for example, secure destruction or transfer to appropriate archives). This vital step will be the basis of your privacy analysis and is essential for determining compliance to legislation, appropriate security safeguards and identifying potential risks. Data flow maps (see example below) are typically accompanied by a Data Flow Table (see 5.3.4) that identifies additional details related to the data flow. Before starting a PIA it is strongly recommended that the appropriate business lead for the initiative be contacted and requested to provide a documented business/work flow as discussed in section 5.2.11.

You are concerned about the flows of PI/PHI and the uses of PI/PHI in context of the flows. Other data flows don't need to be included for PIA purposes, though they may help to provide context. Under either *HIPMA* or *ATIPP*, a "flow" involves a "collection" or "disclosure" of PI/PHI. If a process involves the information moving between different groups within a department this would be considered a "use" of PI/PHI since the actions are within a designated "custodian" (*HIPMA*) or "public body" (*ATIPP*). In the example below, the "flows" are indicated as F1, F2 and F3. The parties involved in the data flow are set out as vertical "swim lanes". Arrows indicate the direction of data flow and connect the collection, use and disclosure steps.

Example: an example data flow map is provided below.



5.3.4 Data Flow Tables

**In the PIA Template refer to section 2.0 “Data Flow Mapping and Tables”*

Along with an accompanying Data Flow Map, a Data Flow Table, which is used to clearly identify compliance with legislation and/or areas of risk, is essential to every PIA. Typically, the table will align to arrows on the associated Data Flow Map and provide details related to:

- the parties involved,
- the purpose of the collection, use or disclosure,
- the mode of data transmission, and
- an analysis of the authority for the data flow, citing applicable legislation,

As noted in 5.3.3 it is imperative that a business process map be obtained to ensure all data flows for the initiative are identified and assessed for risk.

Examples: Below are two possible table formats describing the “F1” flow in the diagram above.

| Personal Information Data Flow Narrative | | | |
|--|---|---|--|
| | Description/Purpose | Data type | Authority |
| 1 | PHI is collected via the CDOP Application form from the individual for the purpose of determining a client’s eligibility to the CDOP program. | Personal Health Information including: <ul style="list-style-type: none"> • Name • Address • Phone Number • PHN | <u>Collection (Direct)</u> <ul style="list-style-type: none"> • Health Care Insurance Plan Act s. 5(j) • Health Care Insurance Plan Act s. 8(1)(i). • Health Care Insurance Plan Act, C.O. 1971/275 s. 8 • HIPMA s. 53(c) <u>Use</u> <ul style="list-style-type: none"> • HIPMA s. 56(1)(j)(i) • HIPMA s. 56(1)(j)(ii) |

| Flow #1: Client submits application to IHHS | |
|---|---|
| Description: | A client visits a provider to receive health care services. If the client is a minor (18 and under) and is part of a low-income family, the provider may recommend that that the client apply for |

| | |
|------------------------|---|
| | the CDOP program. To apply for the program, the client and/or guardian must visit the IHHS office in Whitehorse to complete the application form and submit directly to the Extended Benefits Officer. The Extended Benefits Officer receives the application and photocopies any supporting documentation. This supporting documentation may include previous years' tax returns or a form from Yukon Social Services program to demonstrate the income level of the family. The Extended Benefits Officer then reviews the application to determine if it is eligible for the CDOP program. |
| Purpose: | PHI is collected from the individual for the purpose of determining a client's eligibility to the CDOP program. |
| Data Types | Personal Health Information including name, address, phone number and PHN as collected on the CDOP application form [In this example, the CDOP application form should be attached as Appendix]. |
| Legal Authority | <p><u>Collection (Direct) –</u></p> <ul style="list-style-type: none"> • <i>Health Care Insurance Plan Act s. 5(j)</i> – empowers the director to establish what information is required to be provided to the director under this Act and the form that information must take; • <i>Health Care Insurance Plan Act s. 8(1)(i)</i> – authorizes making regulations to the act providing for the making of claims for payment of the cost of insured health services and prescribing the information which shall be furnished in respect of claims. • <i>Health Care Insurance Plan Act, C.O. 1971/275 s. 8</i> - The Administrator shall have the power to require and receive any and all information that he considers necessary in order to adjudge the claims for services rendered to insured persons by medical practitioners. • <i>HIPMA s. 53(c)</i> – authorizes the collection of personal health information provided that it relates to and is necessary for carrying out a program or activity of a public body or a health care program or activity of a custodian that is a branch, operation or program of a Yukon First Nation. In this case, the provision of health care services in the form of extended benefits, which is an activity of the Yukon Government, cannot be provided without knowing who the individual is, their contact information and their PHN number. <p><u>Use –</u></p> <p><i>HIPMA s. 56(1)(j)(i)</i> – authorizes the use of PHI for the purpose of determining or verifying the individual's eligibility for a program of, or to receive health care or other related goods, services or benefits from, a custodian, if the personal health information was collected in the course of processing an application made by or for the individual.</p> <ul style="list-style-type: none"> • <i>HIPMA s. 56(1)(j)(ii)</i> – authorizes the use of PHI for the purpose of determining or verifying the individual's eligibility for a program of, or to receive health care or other related goods, services or benefits from, a custodian, if the individual is participating in the program or is receiving the health care, goods, services or benefits. |



Remember: You are not alone! Identify and collaborate with experts in your department or organization when conducting a PIA for a new initiative.

5.4 Legislative Analysis

**In the PIA Template refer to Section 1.1.3 and the Table in section 2.1 – under Table Header “Legal Authority”*

Every collection, use and disclosure of personal information requires a legal authority. It is not sufficient that an individual “consents” or voluntarily provides information – there must also be a corresponding legal authority. In addition to providing legal authorities in the data flow table, it may be useful for you to include a brief summary of the legal authorities under which the new activity operates. This analysis will help identify any areas of concern that may require mitigation strategies to be implemented. If in doubt as to what legislation is applicable to an initiative, be sure to consult with the appropriate expert (i.e. legal or privacy) in your department or organization.

5.4.1 HIPMA

The *Health Information Privacy and Management Act (HIPMA)* is a Yukon law that applies to the collection, use and disclosure of personal health information by health information custodians, their agents and information managers.

Schedule 1 of this manual provides a review of the key definitions and sections to consider when conducting a PIA for an initiative subject to *HIPMA*.

5.4.2 ATIPP

Yukon’s *ATIPP* act was enacted to ensure that individuals have the right to access information and to the protection of their privacy in information held by public bodies.

Schedule 2 of this manual provides a review of the key definitions and sections to consider when an analysis is conducted upon an initiative subject to *ATIPP*.

5.4.3 Other

Some government programs have specific enabling legislation that authorizes the program to collect, use and disclose certain PI / PHI. For example, a social assistance program may have enabling legislation that requires individuals to make an application and provide supporting eligibility documentation. Sometimes laws are very specific regarding the information that must be provided (e.g. the forms are prescribed in the legislation) while other times the enabling law may delegate responsibility for determining data collection requirements to a staff position, such as the Program Director. When an assessment is performed on an initiative subject to other legislation besides *HIPMA* and *ATIPP*, it is important to determine which legislation takes precedence when it comes to PI/PHI. This is an area where it would be prudent to seek legal advice and/or consult with program area leaders.




Remember: Documenting the specific legislation and sections in a data flow table assists in conducting the privacy analysis to ensure compliance. It is important to remember to not only cite the legislation and sections that apply, but to also justify how those sections apply. For example, if you are relying on *HIPMA* section 53(c) for the collection of PHI, you must explain the necessity of the information in relation to the program being provided.

5.5 Privacy Analysis

Once information about the initiative has been completed, the privacy analysis can begin. To be effective, this step should be informed by complete and accurate information about the project, as well as by relevant privacy laws, regulations and other compliance requirements. In addition, your department's or organization's practices related to privacy, information management, technology, security and risk management may be relevant to your analysis. Existing policies and procedures, or the lack thereof, can be a significant factor in a department/organization's ability to address privacy risks.

This analysis informs the risk summary and mitigation plan of the PIA. The analysis looks at the extent to which the 10 Principles of the CSA Model Code for the Protection of Personal Information have been met at the time of PIA drafting. If there are gaps, possible mitigation steps will be identified in the Risk Summary table. It will be up to the new program's sponsors to determine if the mitigation steps reduce the risk to an acceptable level.

The sections below include example questions¹² to ask in regards to each of the ten CSA Principles. A more exhaustive set of questions is included in the Detailed Technical and Security Questionnaire in **Schedule 3**. You may wish to refer to the Schedule 3 questionnaire for more complex or technical PIAs.

| | |
|---|---|
|  | <p>Remember: The questions provided in the sections below do not compose an exhaustive list so be sure to go beyond just those listed.</p> |
|---|---|

5.5.1 Principle 1: Accountability

**In the PIA Template refer to section 3.1 "Accountability"*

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

| Questions For Analysis | Yes | No | N/D ¹³ or N/A | Details |
|---|-----|----|--------------------------------|---------|
| 1.1 Has responsibility for the PIA been assigned? Please indicate in the details column the name and position of the person responsible. | | | | |
| 1.2 Has the custody and control of personal information been determined? | | | | |
| 1.3 Has the accountability of the program custodian of personal information been documented? | | | | |
| 1.4 Are the performance requirements of the custodian set out in a measurable way and subject to | | | | |

¹² Series of questions derived from the CSA Model Code for the Protection of Personal Information from a Federal Treasury Board privacy questionnaire and adapted for this manual. The questions prompt yes/no responses. A "N/D" (not determined) response may apply for situations where project planning is at an early stage. An "N/A" (not applicable) can be inserted where questions are not relevant to the subject initiative. The "Details" column is used to explain specifically how a particular requirement is met or why it is not met, and can be used to provide legislative or policy references as applicable.

¹³ N/D: Not Determined (used to flag questions that require additional information); N/A: Not Applicable

| | | | | |
|---|--|--|--|--|
| performance and compliance reviews? | | | | |
| 1.5 Are agents or service providers involved in the custody or control of the personal information? | | | | |
| 1.6 If agents or service providers are involved, do you have a written agreement in place that establishes privacy requirements? | | | | |
| 1.7 Will the Yukon Government be provided with the results of regularly scheduled audits and compliance checks on the privacy requirements of all involved parties? | | | | |
| 1.8 Have applicable policies and procedures been reviewed to ensure the proposal is compliant and, where third parties are involved, to ensure that policies and procedures are coordinated? | | | | |
| 1.9 Have policy or procedure gaps been identified and addressed? | | | | |
| 1.10 Have governance structures been put in place to provide oversight during project development, deployment and operation, including structures for stakeholder input on matters of information governance? | | | | |

5.5.2 Principle 2: Identifying Purposes

**In the PIA Template refer to section 3.2 “Identifying Purposes”*

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

The purpose for the collection of information should be specific and succinctly described in the PIA. If not, ask more questions as knowing the real purpose is critical to ensuring compliance with legislation.

| Questions For Analysis | Yes | No | N/D or N/A | Details |
|--|-----|----|------------|---------|
| 2.1 What is your legal authority to collect personal information? | | | | |
| 2.2 Is the personal information collected directly related to an operating program or activity? | | | | |
| 2.3 Is personal information being collected directly from the individual or their substitute decision maker? If no, why not? | | | | |
| 2.4 If “no” to 2.3 is the personal information collected from another public body (ATIPP) or a custodian (HIPMA)? Is their disclosure authorized in law? | | | | |
| 2.5 Are positive identifiers collected (e.g. social insurance number, driver’s license number, medical record number)? Note in the details if Yukon | | | | |

| | | | | |
|---|--|--|--|--|
| Health Insurance Plan Number is being collected and indicate whether there is specific authority to collect it. | | | | |
| 2.6 Have the purposes for which the personal information is collected been documented? If yes, provide specifics. | | | | |
| 2.7 Is all the personal information collected necessary to the operating program or activity (put another way, is the program collecting the minimum amount of personal information necessary for the program)? | | | | |
| 2.8 Is there notice at the collection stage that identifies the specific purposes for the collection, the authority for doing so and the individual serving as official contact? | | | | |
| 2.9 Is the notice associated with the collection of personal information available and consistent across all mediums of collection? | | | | |
| 2.10 Are secondary uses contemplated for the information collected? If yes, describe them in the details column. | | | | |
| 2.11 If personal information is to be used or disclosed for a secondary purpose not previously identified, is consent required? | | | | |
| 2.12 If consent is not required for secondary purpose use or disclosure, is there authority for the use or disclosure? | | | | |
| 2.13 Is personal information collected from a public database? | | | | |
| 2.14 Will program evaluation, quality assurance or security activities result in the collection of additional personal information? | | | | |
| 2.15 Does the program or activity involve the collection through a common client identifier? If yes, provide details about the identifier. | | | | |

5.5.3 Principle 3: Consent

**In the PIA Template refer to section 3.3 “Consent”*

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except when inappropriate.

| Questions For Analysis | Yes | No | N/D or N/A | Details |
|---|-----|----|------------------|---------|
| 3.1 Is individual consent required for collection, use and disclosure of personal information? If not, why? | | | | |
| 3.2 Is consent obtained directly from the individual? If not, why? | | | | |
| 3.3 Has the form of consent been determined, e.g. no consent, express consent, implied consent? | | | | |
| 3.4 Can the program demonstrate that it meets the legal tests for valid consent (e.g. the consent is knowledgeable, relates to the personal information, given voluntarily, not obtained by fraud or misrepresentation) | | | | |
| 3.4 If express consent is required, has a process for recording the consent been established? | | | | |
| 3.5 If consent is sought, is the form of consent likely to stimulate negative reaction (for example, opt-in or -out)? | | | | |
| 3.6 Can an individual refuse or withdraw their consent to the collection, use or disclosure of their personal information, unless required by law? | | | | |
| 3.7 Would the individual's refusal or withdrawal of consent to the collection, use or disclosure of their personal information disrupt the level of program service provided to the individual? | | | | |
| 3.8 Are standards and mechanisms in place to ensure that the individual has capacity to give consent? | | | | |
| 3.9 Are standards and mechanisms in place to ensure the recognition of persons authorized to make decisions on behalf of others (e.g. a minor or incapacitated person)? | | | | |

5.5.4 Principle 4: Limiting Collection

**In the PIA Template refer to section 3.4 “Collection of Personal Information”*

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

While conducting a PIA, keep alert for terms such as “we’d like to have this information”, “we might need the information”, “it would be nice to have this information in case we need it in future”. These should raise a red flag as they indicate a desire to have the information “just in case”, rather than a legitimate need. Also consider if the information being collected is legitimately needed to meet the purpose. For example, instead of a date of birth, could the initiative collect an age instead and still achieve their purpose? In situations like this you should ask more questions to confirm the data collection will be limited to only what is necessary for the purposes identified in the initiative.

| Questions For Analysis | Yes | No | N/D or N/A | Details |
|---|-----|----|------------|---------|
| 4.1 Has the authority to use personal information been identified? Please indicate the authority. | | | | |
| 4.2 Is personal information used exclusively for the purpose for which the information was obtained or compiled? | | | | |
| 4.3 Are the uses of the information limited to what a reasonable person would consider to be necessary for the purposes of the program? | | | | |
| 4.5 Are personal identifiers used for the purposes of linking across multiple databases? | | | | |
| 4.6 If data matching, is it consistent with the stated purposes for which the personal information is collected? | | | | |
| 4.7 Is information anonymized when used for reporting, planning, forecasting and/or evaluation purposes? | | | | |

5.5.5 Principle 5: Limiting Use, Disclosure and Retention

**In the PIA Template refer to section 3.5 “Use, Disclosure and Retention of Personal Information”*

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

| Questions For Analysis | Yes | No | N/D or N/A | Details |
|---|-----|----|------------|---------|
| 5.1 Will information that the department or | | | | |

| | | | | |
|--|--|--|--|--|
| organization already holds be used for a new purpose? Why and how? | | | | |
| 5.2 What will the new information that the department/organization will be collecting be used for? | | | | |
| 5.3 Will the information be disclosed to outside agencies and if so, through what medium, how often, to whom and for what purpose? | | | | |
| 5.4 Will unique identifiers be assigned and if so why is it necessary? | | | | |
| 5.5 How and where will the information be retained? What security measures will be in place? | | | | |
| 5.6 Will more than one copy of the information be retained and if so, for what purpose? | | | | |
| 5.7 Who will have access to the information and how will that access be managed? | | | | |
| 5.8 Is personal information disclosed by the program other public bodies or custodians? | | | | |
| 5.9 Has the authority to disclose personal information been identified? Please indicate the authority. | | | | |
| 5.10 Is personal information disclosed with the consent of the individual? | | | | |
| 5.11 Are positive personal identifiers disclosed? E.g. social insurance number, medical record number, client ID? | | | | |
| 5.12 Are YHCIP numbers disclosed? | | | | |
| 5.13 Is the personal information to be disclosed limited to the purpose of disclosure? | | | | |
| 5.14 Will personal information be processed, disclosed or retained outside of Canada? | | | | |
| 5.15 Is the personal information scheduled for retention and disposition? Identify the retention policy applies that applies. | | | | |
| 5.16 How will the information be disposed of upon expiry of the retention period and who is responsible to ensure the disposal? | | | | |

5.5.6 Principle 6: Accuracy

**In the PIA Template refer to section 3.6 “Accuracy of Personal Information”*

Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

If personal information is used by a public body to make a decision that directly affects that individual, the public body must make every reasonable effort to ensure that the personal information is as accurate and complete as required for the purpose. This is particularly critical when it comes to health care organizations where a decision based on inaccurate information could lead to disastrous outcomes.

The PIA should describe how an individual’s information will be updated or corrected, including if the request is from the individual themselves. If information that is disclosed to others is changed, the PIA needs to indicate if the other party is notified and how. If no notification is provided, the PIA should also indicate the reasoning for that.

| Questions For Analysis | Yes | No | N/D or N/A | Details |
|--|-----|----|------------|---------|
| 6.1 Will steps be taken to ensure that the personal information is accurate, complete and up-to-date? Please specify. | | | | |
| 6.2 Do records of personal information indicate the date of last information update? | | | | |
| 6.3 Is a record kept of the source of the information used to make changes? | | | | |
| 6.4 Is there a procedure to provide notices of correction to third parties to whom personal information has been previously disclosed? | | | | |
| 6.5 Is there a record kept with respect of requests for a review of errors or omissions and corrections or decisions not to correct? | | | | |
| 6.6 Is there a clearly defined process by which an individual may access, assess and discuss or dispute the accuracy of the record? Please briefly describe the steps | | | | |
| 6.7 Was the information provided directly by the individual or checked by the individual for accuracy? | | | | |
| 6.8 How damaging will it be to the individual if information is wrong or misleading? The more damaging it will be, the more extensive should the steps be for checking accuracy. | | | | |

5.5.7 Principle 7: Safeguards

**In the PIA Template refer to section 3.7 “Safeguarding Personal Information”*

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Without appropriate safeguards, personal information is at risk of unauthorized collection, use, disclosure, retention and disposal, all of which can have significant impacts on the individual whose privacy has been breached, as well as on the organization. Ensuring adequate safeguards to protect personal information is critical to building and maintaining trust and respect with the individuals providing their information.

When conducting a PIA, for each of the safeguards below, consider whether there are vulnerabilities in each part of the information pathway and identify any weak links.

5.5.7.1 Administrative Safeguards

A PIA should identify what, if any, administrative safeguards are in place for the initiative. This would include things such as

- Appropriate user authentication, registration and enrolment procedures
- User training in privacy and security of personal information
- Confidentiality acknowledgements
- Privacy and security policies and procedures, e.g. breach management, audit, individual access & correction (see principle 9), data retention, and consent management
- Contracts, and information sharing agreements

User training in a new software application and its proper usage should also be considered in the analysis. Operational documentation should include privacy best practice content.

5.5.7.2 Technical Safeguards

For initiatives that require new technology, technical safeguards may include organizational network details and a full STRA. For smaller initiatives, a PIA may only need to address more basic technical safeguards related to an application such as user authentication, password complexity and the ability to disable data fields from collecting information. Seek assistance from your Information Technology analyst if needed to complete this section accurately. Some examples of technical safeguards are:

- Unique user identification
- Strong passwords
- Time-based, forced time-outs or log-offs
- Virus protection and firewalls
- Encryption of data
- Data backup and plans for service interruption
- Role-based user access
- Transaction logging and audit reporting
- Encrypted wireless Internet connections

5.5.7.3 Physical Safeguards

Physical safeguards are physical measures used to protect personal information from unauthorized access. Your PIA should note physical safeguards in regards to facility access controls and security, workstation protection, and device and media control. For example:

- Facility/department/office access control
 - Limited access to the building, department or office areas
- Facility security
 - Alarms and security cameras
 - Door locks
 - Identity badges for staff and visitors
- Workstation protection
 - Workstations positioned to avoid shoulder surfing and not viewable to public
- Device and Media control
 - Physical control of portable storage devices such as USB keys and cameras
 - Laptop locks

| Questions For Analysis | Yes | No | N/D or N/A | Details |
|---|-----|----|------------|---------|
| 7.1 Has a Security Threat Risk Assessment (STRA) been completed? | | | | |
| 7.2 Have security procedures for the collection, transmission, storage and disposal of personal information, and access to it, been documented? | | | | |
| 7.3 Are program and information technology staff trained in the requirements for protecting personal information including relevant policies regarding breaches of security or confidentiality? | | | | |
| 7.4 Are there controls in place to grant authorization to modify (add, change or delete) personal information from records? | | | | |
| 7.5 Is the system designed so that access and changes to personal information can be audited by date, action, client and user identification? | | | | |
| 7.6 Are user accounts, access rights and security authorizations controlled by a system or record management process? | | | | |
| 7.7 Are access rights only provided to users on a “need to know basis” consistent with the stated purposes for which the personal information was collected? | | | | |
| 7.8 Is there an inventory of information assets, including sensitivity ratings? | | | | |
| 7.9 Are security measures commensurate with the | | | | |

| | | | | |
|---|--|--|--|--|
| sensitivity of the information recorded? | | | | |
| 7.10 Are there documented procedures in place to identify and respond to privacy or security breaches (disclosures of personal information in error)? | | | | |
| 7.10 Is there an applicable user access auditing policy and procedure? | | | | |
| 7.11 Is there a plan to assess the ongoing state of the safeguards applicable to the system? | | | | |
| 7.12 Are laptop cables and locks used to prevent theft? | | | | |
| 7.13 Are portable devices secured when not in use? | | | | |
| 7.14 Are printers /fax machines located in a secure area not accessible to the public? | | | | |
| 7.15 Are ID badges visible on staff and visitors? | | | | |
| 7.16 Does the application have a time-out configured, and if so what is it set to? | | | | |
| 7.17 Is there an automatic lock of the computer after a set period of time? If yes, what time period? | | | | |
| 7.18 Are hard drives in computers encrypted? | | | | |
| 7.19 Are mobile devices (USB, laptops) encrypted? | | | | |
| 7.20 Is two factor authentication used for remote access to the system? | | | | |
| 7.21 Is wireless networking used? If so does it meet organizational requirements for encryption? | | | | |
| 7.22 Is there a password policy/procedure in place that enforces complexity, length and regular changing of the password? | | | | |
| 7.23 If application has a vendor set Admin password, has it been changed? If not, why not? | | | | |

5.5.8 Principle 8: Openness

**In the PIA Template refer to section 3.8 “Openness”*

An organization shall make readily available to individuals’ specific information about its policies and practices relating to the management of personal information.

Individuals have a right to know an organization’s policies and practices as they relate to the management of personal information. If your organization has publicly posted policies online that should be noted in the PIA. If not, then the PIA should document the process in place should an individual request information on the organization’s management of personal information.

| Questions For Analysis | Yes | No | N/D or N/A | Details |
|--|-----|----|------------------|---------|
| 8.1 Will the results of any privacy impact assessment or audit be communicated outside the program area, including the Office of the Information Privacy Commissioner? | | | | |
| 8.2 Are policies and practices relating to the program's management and handling of personal information available to the public? | | | | |
| 8.3 Is there a communications plan and defined process for communicating with the public about how personal information will be managed and protected? | | | | |
| 8.4 Where appropriate, have key stakeholders been provided with an opportunity to comment on the privacy protection implications of the proposal? | | | | |
| 8.5 Where appropriate, will public consultation take place on the privacy implications of the proposal? | | | | |

5.5.9 Principle 9: Individual Access

**In the PIA Template refer to section 3.9 "Individual Access to Personal Information"*

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

A PIA should clearly indicate whether or not your department/organization's has a process in place for an individual to request access to their records, as well as a process for an individual to request changes to information in their record.

| Questions For Analysis | Yes | No | N/D or N/A | Details |
|--|-----|----|------------------|---------|
| 9.1 Is the program designed to ensure that an individual can have access to his/her personal information, including all other programs or applications that have received copies of the information? | | | | |
| 9.2 Is the program designed to ensure that an individual has been notified that a correction to his/her information has been made? | | | | |
| 9.3 Are all program participants aware of an individual's right of access and the complaint | | | | |

| | | | | |
|---|--|--|--|--|
| process? | | | | |
| 9.4 Are there documented procedures on how to initiate privacy requests or requests for the correction of personal information? | | | | |
| 9.5 Is there a documented process for providing individuals “routine” access to their personal information? | | | | |

5.5.10 Principle 10: Challenging Compliance

**In the PIA Template refer to section 3.10 “Challenging Compliance”*

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Individuals have a right to challenge how their information is managed by an organization, and a PIA should identify the process for this, including who to contact within the organization, and contact information for the Yukon Information & Privacy Commissioner.

| Questions For Analysis | Yes | No | N/D or N/A | Details |
|--|-----|----|------------|---------|
| 10.1 Is there a documented complaint procedures for the program that is consistent with legislated requirements? | | | | |
| 10.2 To improve information management practices and standards, has a procedure been established to log and periodically review the nature, frequency and resolution of complaints? | | | | |
| 10.3 Are there oversight and review mechanisms implemented or available to ensure privacy and security accountability? | | | | |
| 10.4 Have oversight agencies, including the Office of the Information Privacy Commissioner, issued reports or opinions on applicable issues that have been reviewed as part of this program? Provide applicable details. | | | | |

6.0 Assessing Risk & Mitigation Strategies

**In the PIA Template refer to section 4.0 “Overall Risk and Mitigation”*

The risk summary and mitigation plan are essential components to the PIA to enable the Executive Sponsor(s) to decide whether or not to approve the PIA so the initiative can proceed as scheduled. This component also provides details needed for entry into your department/branch Risk Registry.


Upon completion of the privacy analysis, a table is typically included in a PIA that identifies risks to personal information, along with their likelihood of happening and their impact should they occur, along with associated mitigation strategies. Timelines for completion and identifying the party responsible may also be included in the table. Note that determining the level of risk should be done collaboratively with the business sponsor and is not the sole responsibility of the PIA author.

7.0 PIA Reviews and Approvals

**In the PIA Template refer to section 5.0 “Comments from Reviewer” and section 6.0 “Signatories and Approval”*

Once the PIA is fully drafted, it is time to send it out for review and feedback. Who reviews a PIA may vary depending on the initiative, but should always include your department Privacy Officer. For a small project that impacts one department it may be just a business sponsor, department Privacy Officer and the ATIPP Office reviewing it, whereas for a project that may impact all departments of government there may be a large number of reviewers such as legal, department privacy officer, business leads, and subject matter experts, with multiple iterations of reviews being necessary before all parties are satisfied that the assessment is complete and ready for final approval.

Remember that regardless of the initiative, as per the Yukon Government PIA Operational Policy, all PIAs must be submitted to the ATIPP office for review and comment within a reasonable time frame prior to launch and must be signed to be considered complete. If a PIA is required to be submitted to the OIPC for review, a representative from the ATIPP office should be present when a department meets with the OIPC to receive comments on a submitted PIA unless approved by the Director of Corporate Information Management.

| | |
|---|--|
|  | <p>Remember: the HIPMA general regulation requires the Health and Social Services Department and the Yukon Hospital Corporation to submit privacy impact assessments to the Yukon Information & Privacy Commissioner before the initiative goes live.</p> |
|---|--|

8.0 PIA Addendums

**This section is not identified in the current PIA Template – include this section as required*

A PIA is a living document. While the initial PIA may be approved, it is critical that ongoing changes to the initiative be documented and re-assessed as new risks may arise if changes are implemented. Changes to scope, business owner, legislative or regulatory authority, business processes, partners or third party service providers, technology, functionality, service delivery model, security and information requirements may create new privacy risks and trigger the need to update the original privacy analysis and mitigation strategy documented in the original PIA. As well, mitigation strategies from the original PIA may be completed thereby reducing risk, so ensuring that PIAs are reviewed and updated regularly is imperative to remaining diligent in protecting personal information and ensuring compliancy with legislation.

Most updates to a PIA can be done through Addendums. However, if there are significant changes from the original PIA such as an upgrade to an existing system that introduces new functionality or new data collection, then a new PIA may be necessary.

Consider scheduling regular reviews of your department's/organization's PIAs as a proactive way to ensure the protection of personal information and compliance with policies and legislation.



Remember: Be proactive and conduct regular reviews of completed PIAs to ensure accuracy and avoid unexpected privacy breaches.

Schedule 1: Health Information Protection and Management Act (HIPMA) Summary

The *Health Information Privacy and Management Act (HIPMA)* is a Yukon law that applies to the collection, use and disclosure of personal health information by health information custodians, their agents and information managers.

The Act includes:

- Requirement to not collect, use or disclose personal health information if other information will suffice;
- Requirement to not collect, use or disclose any more personal health information than is necessary for the purpose;
- Restrictions on collecting public health insurance plan numbers;
- Obligations to have documented privacy procedures;
- Designating a privacy contact person; and
- Making Statements of Information Practices public.

Definitions: the following definitions apply:

- “health care” is defined in the Act to mean any activity (other than an activity that is prescribed not to be health care) that is or includes (a) any service (including any observation, examination, assessment, care, or procedure) that is provided to i) diagnose, treat or maintain an individual’s physical or mental condition;
- The Health and Social Services Department is specifically defined as a “custodian” in the Act;
- “health information” and “personal health information” of an individual means identifying information of the individual, in unrecorded or recorded form, that (a) relates to the individual’s health or the provision of health care to the individual.

Application of the Law: Section 7(2)(c) and (d) states that the act does not apply to PHI (or a record containing PHI) that is prescribed (i.e. is specifically addressed in another law) or that is collected, used or disclosed in prescribed circumstances or for a prescribed purpose. This section means that *HIPMA* may not apply in situations where another law provides a specific authorization for a collection, use or disclosure of PHI. For example, health care providers submit patient health information to the Insured Health and Hearing Services (IHHS) Branch of HSS in the form of medical claims and applications for medical travel as authorized under the *Health Insurance Plan Act* and the *Travel for Medical Treatment Act*.

Minimum PHI: Section 16 states that the collection, use and disclosure of PHI by a custodian or their agent must be limited to the minimum amount of PHI that is reasonably necessary to achieve the purpose for which it is collected, used or disclosed.

Information Practices: Section 19 states that a custodian must protect personal health information by applying information practices that include administrative policies and technical and physical safeguards that ensure the confidentiality, security, and integrity of the personal health information in its custody or control. It is important that these policies and procedures be documented (as opposed to being just being applied by convention) to ensure consistent practice.

With respect to information practices the custodian must:

- Implement measures that protect the confidentiality, privacy, integrity and security of personal health information and prevent its unauthorized modification (s. 19(3)(a));
- Implement controls that limit the individuals who may use personal health information to those specifically authorized by the custodian to do so (s. 19(3)(b));
- Implement controls to ensure that personal health information cannot be used unless (i) the identity of the individual seeking to use the personal health information is verified as an individual the custodian has authorized to use it, and (ii) the proposed use is authorized under this Act (s. 19(3)(c));
- Take all reasonable steps to prevent a security breach (s. 19(3)(d));
- Provide for the secure storage, disposal and destruction of records to minimize the risk of unauthorized access to, or disclosure of, personal health information (s. 19(3)(e));
- Develop policies which provide that personal health information is retained in accordance with the prescribed requirements, if any (s. 19(3)(f));
- Establish a procedure for receiving and responding to complaints regarding its information practices (s. 19(3)(g)); and
- Meet the prescribed requirements, if any (s. 19(3)(h)) – for example requirements that may be set out by regulation (s.14).

Privacy Contact: A custodian must designate a “contact individual” for the following functions (s. 20(2)):

- a) receive and process complaints from the public about the custodian’s information practices;
- b) respond to requests for access to, or correction of, a record of an individual’s personal health information that is in the custody or control of the custodian;
- c) ensure that all agents of the custodian are appropriately informed of their duties under this Act;
- d) respond, in respect of security breaches, to individuals whom the custodian has notified under section 30 and to the commissioner; and
- e) perform any prescribed functions or duties.

Information Practices: A custodian must make a written statement of information practices available to the public. This statement must include a general description of the custodian’s information practices and contact details. It must describe how an individual can make a request to access their information, and make a complaint to the custodian or commissioner (s. 21)

Disclosure Record: Under section 22(1) custodians are required to keep a record of disclosures of PHI that were done without the individual’s consent.

Access Audit Logging: A custodian must create and maintain (or cause to be created and maintained) for any electronic information system the custodian uses to maintain personal health information, a record of user activity that includes, in respect of each incident of access by a person, through the system, to personal health information or personal information (s. 22(3)).

Right to Access: Individuals have the right to access the personal health information held about them. Individuals may make a request and expect a response from the custodian or their agent as described in the Act, Section 24-25.

If a custodian uses electronic means to collect, use or disclose an individual's personal information, the user's right of access includes a copy of a record of user activity of the individual's personal health information (s. 24(3)). This drives a requirement for user access audit logging (and retention of log files).

Unless extended for specified reasons, a custodian has 30 days to respond to an individual's request for access (s. 26(1)). The detailed steps for responding to (or refusing) an access request are set out in sections 26 and 27.

Individuals may request that changes be made to their records. The Act describes the steps to be taken in Section 28.

Security Breaches: An information security breach is the loss, theft, disposition or disclosure, or access by a person contrary to this Act or a regulation. If it is reasonable to believe that a security breach has occurred and there is risk of significant harm as a result, the custodian must notify the individual as soon as reasonably possible. The process for determining whether the individual is in "significant harm" is outlined in section 30(2). In the notice, the custodian must:

- Describe the circumstances of the breach;
- Indicate when the breach occurred;
- Describe the measures, if any, that the custodian has taken to reduce the risk of harm to the individual as a result of the breach, and
- Identify the custodian's contact individual.

The Information Privacy Commissioner of Yukon must be notified in all cases deemed significant enough to inform the individual. The commissioner must be given a copy of the notice sent to the individual.

Consent: Sections 32 to 40 set out requirements related to individual consent. The following are summary points related to consent:

- Implied consent for collection, use or disclosure of PHI is generally sufficient (s. 33);
- Express consent is required for fundraising or other prescribed purposes. Express consent does not need to be in writing but must be recorded by the custodian (s. 34, 35);
- Custodians must, with some exceptions, accommodate situations where an individual refuses, withdraws, or places a condition on consent (s. 36)
- To be valid, consent must (s. 38):
 - Be knowledgeable;
 - Relate to the PHI; and
 - Be given voluntarily and not be obtained by fraud or misrepresentation.
- An individual's consent to the collection, use or disclosure of their personal health information is knowledgeable only if the individual knows (s. 39)
 - The purpose of the collection, use or disclosure of their PHI;
 - That they may give, withhold or later withdraw their consent.
- A custodian is generally entitled to assume the following regarding consent (s. 40):
 - That the individual is capable of giving consent regardless of their age;
 - That the consent for purposes of providing health care is knowledgeable;
 - That documented consent is valid;
 - That the individual has not withdrawn their consent.

- If an individual refuses to give consent, or withdraws consent, to a custodian's collection, use or disclosure of the individual's personal health information for the purpose of providing health care to the individual, the custodian must (s. 43):
 - Inform the individual of the reasonably foreseeable consequences of the refusal or withdrawal;
 - Take reasonable steps to act in accordance with the decision; and
 - Where the individual has withdrawn consent, upon request of the individual make reasonable efforts to inform the individual of the identity of each other person to whom the custodian has, during the year before the custodian received the individual's request, disclosed the personal health information.
- A custodian may refuse to comply with an individual's consent directive if the custodian reasonably believes compliance is likely to endanger the individual's health or safety (s. 43).

Notice: A custodian is entitled to assume that an individual's consent to the collection, use or disclosure of their PHI is knowledgeable if the custodian has posted a notice in a place where it is likely to come to the individual's attention, or makes such a notice readily available to the individual (s. 41). The notice must:

- Describe the purpose of the collection, use or disclosure;
- Advise that the individual may give or withhold consent and having once given consent, may withdraw that consent;
- Confirm that without the individual's consent the personal health information can be collected, used or disclosed only in accordance with the provisions of this Act and the regulations; and
- Advise that if the personal health information is disclosed outside Yukon, the law of the jurisdiction to which it is disclosed will govern its use, collection and disclosure in that jurisdiction.

Capacity: Section 45 sets out custodian requirements with respect to capacity of individuals to give consent.

Collection: Part 6 - Division 2 of the Act addresses collection of PHI. Of particular note, a custodian may collect an individual's PHI only if:

- The custodian has the individual's consent;
- The collection is authorized by law; or
- The collection relates to and is necessary for carrying out a program or activity of a public body or a health care program or activity of a First Nation custodian.

Use: Part 6 - Division 3 of the act addresses the use of PHI. Section 55 addresses "use with consent" and section 56 addresses "use not requiring consent".

A custodian may use an individual's PHI that is in its custody or control:

- For the purpose of providing health care to the individual (unless the individual has refused or withdrawn consent); or
- For any other lawful purpose if the individual consents to the use.

A custodian may without the individual's consent use an individual's PHI that is in its custody or control (not an exhaustive list):

- For the purpose of preventing or reducing a risk of serious harm to the health or safety of any other individual;
- For the purpose of assembling a family or genetic history of the individual;
- For the purpose of educating agents of the custodian in respect of the provision of health care;
- For the purpose of modifying (including removing identifying information from), destroying or disposing of the information;
- For the purpose of assessing or confirming an individual's capacity;
- For the purpose of managing or auditing the health care activities of the custodian; and
- For the purpose of carrying out quality improvement.

The Minister, the Department, the Yukon Hospital Corporation or a prescribed branch, operation or program of a public body may, without an individual's consent, use the individual's PHI for the purpose of the planning and management of the health system.

Disclosure: Part 6 - Division 4 addresses the disclosure of PHI. Section 57 sets out the requirements for "disclosure with consent", while section 58 addresses "disclosure not requiring consent".

*HIPMA General Regulation*¹⁴

The *HIPMA* General Regulation came into force on August 31, 2016.

The definition of PHI is expanded under section 8 and 9 to include the registration information for the individual and includes:

- Name
- Residential address
- Telephone number
- Email address
- Substitute decision maker

Sections 12 and 13 place limitations on the collection and use of an individual's health insurance plan number.

Section 14 sets out specific information practices required of custodians, who must:

- Determine the PHI that their agents are authorized to access;
- Ensure that their agents sign a pledge of confidentiality;
- Provide agents with privacy and security training;
- Have written policies in relation to:
 - collection, use and disclosure of PHI;
 - security breach management;
 - individual's access to records
- Conduct a security audit at least every two years;

¹⁴ <http://www.hss.gov.yk.ca/pdf/hipma-regs.pdf>

- Ensure security of movable media;
- Ensure appropriate PHI security safeguards;
- Limit physical access to designated areas containing PHI;
- Ensure there is a record created for all security breaches;
- Address the privacy and security risks of an agent's remote access to the custodian's information systems.

Section 15 requires HSS to conduct a privacy impact assessment before:

- Implementing any measure that in the opinion of the Minister is a significant change to an existing information system that processes PHI; or
- Commencing the operation of a new information system that processes PHI.

A PIA conducted under section 15 must be submitted to the Privacy Commissioner prior to launch.

The regulation in section 16 defines the functions and duties of a custodian's contact individual. These include:

- Facilitating the custodian's compliance with the Act;
- Assisting individuals who wish to make a complaint about the custodian;
- Facilitating custodian staff education regarding the Act.

Sections 17 to 20 deal with consent. Additional requirements for public notices (the basis for informed consent as required in section 41(1) of the Act) are set out in section 17. Notice must:

- Be in writing;
- Be in English or French;
- Be expressed in plain language; and
- Generally, describe the custodian's record retention schedule.

If the custodian refuses to comply with an individual's refusal or withdrawal of consent, the custodian must inform the individual of their right to make a complaint to the Privacy Commissioner (s. 18).

The requirement for express consent is set out in section 19 – where the purpose is research, marketing or communication to the public media.

An individual wishing to withdraw their consent to a custodian's collection, use or disclosure of PHI must do so in writing (s. 20).

Section 21 addresses a custodian's written agreement to use an information manager.

Section 24 sets out the conditions for a custodian's disclosure of PHI for law enforcement purposes.

Sections 27 to 32 deal with fees for individual access to PHI. Selected details:

- There is no requirement to charge a fee. However, if a fee is charged it must comply with the maximum amounts set out in section 29;
- No fee can be charged for transferring an individual's health record to another custodian who is assuming care responsibilities for the individual (s. 30);
- No fee can be charged for responding to a request for a record of user activity (s. 31); and

- Procedures for responding to a request for an estimate of fees are set out in section 32.

Under section 34, the commissioner is authorized to review and comment on any PIA submitted.

Yukon Health Information Network (YHIN) Regulation¹⁵

The YHIN regulation sets out requirements for designated YHIN systems.

Section 4 states that the minister may identify a specified system as being part of YHIN and designate a person as the administrator of the specified system.

Section 5 states that the minister may by order approve the implementation of any form of masking for a specified system. An individual may (s. 6) make an application in writing to a designated HSS office to have their information masked in a YHIN system. Under section 7, the specific YHIN system administrator (e.g. the designated Meditech administrator) would then “as soon as practicable and to the greatest extent reasonably possible given the technical capacities of the specified system and the administrator’s resources, give effect to the masking, or the modification or removal of masking, that the application requests”.

¹⁵ <http://www.hss.gov.yk.ca/pdf/hipma-yhin-regs.pdf>

Schedule 2: Access to Information and Protection of Privacy Act (*ATIPP*)

Summary

Purpose

The purpose of Yukon's *ATIPP* act is to ensure that individuals have the right to access information and to protection of their privacy in information held by public bodies.

The act guarantees certain fundamental rights for individuals including:

- Access to records in the custody and control of Yukon government departments and designated public bodies with certain exceptions (see below);
- Access to individuals own personal information and the right to request correction of errors;
- Privacy of personal information in the custody or under the control of public bodies;
- Protection against unauthorized collection, use, disclosure, or disposition of personal information; and
- Independent review of decisions made by public bodies about access and privacy.

Application

The *ATIPP* act applies to all records in the custody or under the control of a public body, including court administration records, but does not apply to the following (Sec.2):

- Court records or judicial notes, administration records, or records of the support services provided to the judges of those courts;
- Personal notes, communications, or draft decisions of a person who is acting in a judiciary capacity;
- Records of the legislative assembly;
- Records of questions that are to be used on an examination or test;
- Materials placed in Yukon Archives by or for a person or agency other than a public body;
- Information published by a public body and still available for purchase or access by the public; or
- A record containing teaching material or teacher information of employees of the Yukon College.

Personal Information

Personal Information (PI) is defined by the *ATIPP* (Sec.3) as recorded information about an identifiable individual, including:

- A person's name, address, or telephone number;
- Demographic information (age, height, race, religion, marital status, sexual orientation etc.);
- An identifying number, symbol, or other particular assigned to the individual;
- The individual's fingerprints, blood type, or inheritable characteristics;
- Information about the individual's health care history, including a physical or mental disability;
- Information about the individual's educational, financial, criminal, or employment history;
- Anyone else's opinions about the individual; and
- The individual's personal views or opinions, except if they are about someone.

ATIPP differs from other information privacy acts, as it includes the contact information of an individual under the definition of PI.

Collection

Sec. 29 of the act states that no personal information may be collected unless:

- The collection of that information is authorized by an act of parliament or the legislature;
- The information is collected for the purposes of law enforcement; or
- That information relates to and is necessary for carrying out a program or activity of the public body.

The *ATIPP* does not specifically speak to collection of information for the purposes of evaluation or a program. It could be argued that the evaluation of a program is necessary for carrying out the program, and therefore covered under Subsection C.

Direct Collection

(Sec. 30) A public body must collect personal information directly from the individual the information is about unless:

- Another method of collection is authorized by:
 - That individual;
 - The Information and Privacy Commissioner; or
 - An Act of Parliament or of the Legislature.
- The information is collected for the purpose of:
 - Determining suitability for an honour or award;
 - A proceeding before a court or a judicial or adjudicative body;
 - Collecting a debt or making a payment; or
 - Law enforcement.

Use

Under sec. 35(1), a public body may use personal information only:

- For the purpose for which that information was obtained or compiled, or for a use consistent with that purpose;
- If the individual the information is about has consented to the use; or
- For the purpose for which that information may be disclosed to that public body under sections 36 to 39.

A public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner.

Disclosure

Under sec. 36, disclosures may only occur:

- If the disclosure is made under the authority of the Part 2 of the act;
- If the individual the information is about has consented;

- For the purpose for which it was obtained or compiled or for a use consistent with that purpose;
- For the purpose of complying with an enactment of, or with a treaty, arrangement or agreement made under an enactment of Canada or the Yukon;
- For the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information
- To an officer or employee of the public body or to a Minister, if the information is necessary for the performance of the duties of the officer, employee or Minister;
- To the legal counsel for the Government of the Yukon or its insurers for use in civil proceedings involving the Government;
- For the purposes of the Coroners Act, or the Public Guardian and Trustee's functions under the Public Guardian and Trustee Act; or
- Other circumstances as outlined in Section 36

Disclosure for Research or Statistical Purposes

Under sec. 38, a public body may disclose personal information for a research purpose, including statistical research, only if:

- a. The research cannot reasonably be accomplished unless that information is provided in individually identifiable form;
- b. Any link between the record and any other records is not harmful to the individuals that the information is about and the benefits to be derived from the record linkage are clearly in the public interest;
- c. The public body concerned has approved conditions relating to:
 - i. Security and confidentiality;
 - ii. The removal or destruction of individual identifiers at the earliest reasonable time;
 - iii. The prohibition of any subsequent use or disclosure of that information in individually identifiable form without the express authorization of that public body; and
- d. The person to whom that information is disclosed has signed an agreement to comply with the approved conditions, this Act and any of the public body's policies and procedures relating to the confidentiality of personal information.

Access and Correction

Under sec. 32, a person may request a correction to information held about them by a public body if they believe there is a mistake. They may make this request to the records manager. If no correction is made, the record must be annotated with the correction that was requested but not made. If a correction is made, the public body must give notice of the correction to any public body or third party to whom the information was disclosed.

If a request for information is denied, the individual may make a request for the Privacy Commissioner to review (Sec, 48).

The Information and Privacy Commissioner

The Ombudsman appointed under the Ombudsman Act is also the Information and Privacy Commissioner (Sec. 40(1)), and the acting Ombudsman is also the acting Privacy Commissioner. General powers (Sec. 42) of the Privacy Commissioner may:

- a. Inform the public about the Act
- b. Receive complaints or comments from the public concerning the Act, conduct investigations into those complaints and report on those investigations;
- c. Comment on the implications for access to information or for protection of privacy of existing or proposed legislative schemes or programs of public bodies;
- d. Authorize the collection of personal information from sources other than the individual the information is about;
- e. Report to a Minister information and the commissioner's comments and recommendations about any instance of improper administration of the management or safekeeping of a record or information in the custody of or under the control of a public body.

The Privacy Commissioner must report to the legislation annually (Sec. 47).

Schedule 3: Detailed Technical and Security Questionnaire

The following is a detailed questionnaire that provides additional guidance with specific technical and security-related issues. Note that some sections will not be applicable for all PIAs. Remember to consider the scope of your PIA and choose the relevant questions to address.

| # | Heading | Question |
|------------------------|--------------|--|
| Risk Management | | |
| 1 | General | Has the organization identified what personal information assets are being held, and their sensitivity? |
| 2 | Risk Reviews | Has the organization conducted a security threat risk assessment (STRA)? |
| 3 | Risk Reviews | Are risk assessments conducted at planned intervals to review the residual risks and the identified acceptable levels of risks and account for technical, business or legal changes? |
| 4 | Risk Reviews | When the organization identifies changes to risks, is the focus and/ or priority placed on the most significantly changed risks and their associated preventive action requirements? |
| 5 | Risk Reviews | Is there a process trigger for when a non-scheduled TRA or Privacy Impact Assessment (PIA) is required (e.g. security or privacy incident, new threats)? |
| Policies | | |
| 6 | General | Do operational security policies exist? (For example, policies around secure faxing of personal information, policies and procedures for end-of-day closing, policies for using couriers to send personal information and/or policies for reviewing audit logs.) |
| 7 | General | Have the operational security policies been endorsed by management? |
| 8 | General | Has the responsibility for reviewing and updating the organization's policies, procedures, guidelines and standards been defined and assigned? |
| 9 | General | Is the personal information security policy reviewed at planned intervals, or if significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness? |
| 10 | General | Are independent reviews of the security policies carried out on a regular basis to ensure compliance with current legislative standards? |
| 11 | General | Are organizational policies and standards updated as a result of this review? |
| 12 | General | Can the security officer responsible for the policy update the policy and republish it to the organization? |
| 13 | General | Do employees, contractors and partners have easy access to the personal information security policy? |
| 14 | General | Does the public have access to information about the organization's personal information security policy? |
| 15 | General | Do incentives exist for employees, contractors, customers and partners to understand and follow the policy? |
| 16 | General | Does the organization track acceptance and measure awareness of security policies? |
| 17 | General | Is there a policy for hardware maintenance and upgrades? |
| 18 | General | Is there a network security infrastructure policy that includes a copy of a current network diagram? |
| 19 | General | Does the network security policy require that system security documentation be protected from unauthorized access? |
| 20 | General | Is there a policy controlling or prohibiting hardware and software not purchased or supported by the organization and their use on the network? |
| 21 | General | If personal information is collected over the Internet, is there a specific policy to manage this practice? |

| # | Heading | Question |
|---------------------------|-------------------------------------|--|
| 22 | General | Is there a policy that governs access to personal information and IT assets, networks and systems from outside the organization (e.g. remote working, teleworking)? |
| 23 | General | Is there a policy concerning travelling with personal information? |
| 24 | General | Is there an acceptable use policy? |
| 25 | General | Are there policies and appropriate security controls in place governing electronic mail, instant messaging, social networks, blogs, and so on? |
| Records Management | | |
| 30 | Information Classification | Is there an information classification policy? |
| 31 | Information Classification | Does the information classification policy clearly outline how personal information is to be handled and protected? |
| 32 | Information Classification | Have an appropriate set of procedures for information labelling and handling been developed and implemented to support the information classification scheme adopted by the organization? |
| 33 | Information Classification | Are users informed of any applicable privacy legislation and repercussions of improper classification? |
| 34 | Retention of personal information | Have specific retention periods been defined for all personal information (and in accordance with various legal, regulatory or business requirements)? |
| 35 | Destruction of personal information | Is personal information contained on obsolete electronic equipment or other assets securely destroyed before the equipment or asset is disposed of? For example, are the internal hard drives of faxes and printers properly disposed of when replacing old equipment? |
| 36 | Destruction of personal information | Are hard copy records containing personal information shredded, mulched or otherwise securely destroyed when no longer required for retention? |
| 37 | Destruction of personal information | Is personal information on magnetic media destroyed by overwriting, degaussing or using some other approved method? |
| 38 | Destruction of personal information | Are the contents of erasable storage media containing personal information obscured using an appropriate technique before the medium is reused? |
| Human Resources | | |
| 39 | Executive Leadership | Does management actively support personal information privacy and security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of personal information security responsibilities? |
| 40 | Executive Leadership | Is there a management-level employee (and management-level contractor representative, where a contract is in place) identified as responsible for privacy and security practices? |
| 41 | Training | Has training been implemented for all employees, data custodians and management to ensure they are aware of and understand their security responsibilities? |
| 42 | Training | Is annual privacy and security training a requirement for any handling of personal information? |
| 43 | Training | Are there consequences, such as blocking access to personal information, if employees do not complete annual privacy and security training? |
| 44 | Training | Are there consequences for compromising keys, passwords and other security policy violations? |
| 45 | Training | Is completion of privacy and security training tracked? |
| 46 | Confidentiality Agreements | Are employees required to sign confidentiality agreements? |

| # | Heading | Question |
|--------------------------|----------------------------------|--|
| 47 | Confidentiality Agreements | Do the agreements clearly define individual responsibilities for security, including the protection of personal information? |
| 48 | Confidentiality Agreements | Is responsibility for security an integral part of an individual's annual performance objectives? |
| 49 | Hiring and Terminations | Are potential employees who will have access to personal information adequately and appropriately screened? |
| 50 | Hiring and Terminations | Is there a process to ensure immediate recovery of keys and pass cards, and the revocation of access privileges and appropriate notification of security personnel when a termination (voluntary or involuntary) occurs? |
| 51 | Contractors and Third Parties | Are private sector organizations and individuals who have access to personal information adequately and appropriately screened? |
| 52 | Contractors and Third Parties | Are the necessary privacy and security requirements specified in any contractual documentation? |
| 53 | Contractors and Third Parties | Are contractors required to comply with the organization's privacy and security policies or equivalent policies to ensure that contractors are bound by the same legislated privacy standards as the organization? |
| 54 | Contractors and Third Parties | Are security controls in place to govern the activities of contractors, customers and partners who may have access to the organization's systems and data? |
| 55 | Contractors and Third Parties | Does a knowledgeable employee supervise external hardware or software maintenance personnel whenever maintenance is undertaken? |
| 56 | Contractors and Third Parties | Are contractors and other third parties required to securely destroy or return personal information to the contracting organization upon completion of the contract? |
| 57 | Contractors and Third Parties | If not required to return the information, are contractors and other third parties required to securely destroy, using an approved method, the information at the completion of the contract? |
| Physical Security | | |
| 58 | General | Do physical security measures used for storing personal information include: locked cabinets, locked doors, pass cards, intrusion alarms? |
| 59 | General | Is there a secure area for servers containing personal information ensuring walls extend from the floor to ceiling? |
| 60 | General | Is there a secure area for servers containing personal information ensuring physical access is restricted to authorized personnel? |
| 61 | General | Is there a secure area for servers containing personal information ensuring accesses to the secure space are logged and routinely reviewed? |
| 62 | General | Is there a secure area for servers containing personal information ensuring visitors are escorted by an authorized individual while in the secure space? |
| 63 | General | If any personal information is stored on local hard drives, is that equipment bolted to the floor? |
| 64 | General | Are publicly accessible service counters kept clear of personal information? |
| 65 | General | Is there a nightly security closing protocol? |
| 66 | General | Are access points such as delivery and loading areas and other points where unauthorized persons may enter the premises controlled? |
| Systems Security | | |
| 67 | Terminals and Personal Computers | Are terminals and personal computers used for handling personal information positioned so that unauthorized personnel cannot see their screens? |

| # | Heading | Question |
|-------------------------|----------------------------------|---|
| 68 | Terminals and Personal Computers | Are terminals and personal computers used for handling personal information positioned so that they are not readily visible from outside the facility? |
| 69 | Terminals and Personal Computers | If a user walks away from his or her terminal, is there an automatic process to lock out all users after a defined period of inactivity (e.g. screensaver requiring the authorized user to log on again)? |
| 70 | Mobile and Portable Devices | Is there a policy governing the use of mobile devices and removable media if personal information is stored on them? |
| 71 | Mobile and Portable Devices | Is the policy reviewed and updated on a regular basis? |
| 72 | Mobile and Portable Devices | Does the policy require that the least amount of personal information be stored on the device? |
| 73 | Mobile and Portable Devices | Is personal information encrypted when stored on mobile and portable devices, as well as on removable media? |
| 74 | Mobile and Portable Devices | Is personal information deleted from mobile and portable devices as soon as possible? |
| 75 | Mobile and Portable Devices | Are there reasonable controls in place to prevent the theft of mobile computing and portable devices when left unattended? |
| 76 | Mobile and Portable Devices | Are controls in place to prevent or restrict the connection of personal mobile devices (e.g. smartphones) or removable media (e.g. USB drives) to the organization's networks and systems? |
| 77 | Mobile and Portable Devices | Where mobile or portable devices are allowed to connect to the organization's networks or systems, are they checked to ensure that appropriate security controls (e.g. firewall, anti-virus software) are installed and correctly configured? |
| 78 | Mobile and Portable Devices | Are removable media used to store personal information stored in secure containers when not in use? (e.g. locked in a secure cabinet) |
| 79 | Mobile and Portable Devices | Are laptops containing personal information cable-locked to desks when in use or otherwise equipped with an alarm that will sound if an attempt is made to remove the laptop? |
| 80 | Mobile and Portable Devices | If equipment such as a laptop computer is removed from the premises on a temporary basis by staff, are control procedures in place to record the removal information? |
| 81 | Mobile and Portable Devices | Is laptop encryption prevented from being disabled by the user? |
| 82 | Mobile and Portable Devices | Are laptops equipped with a mobile device management system? |
| 83 | Mobile and Portable Devices | Are laptops configured so that users are prevented from changing security settings or downloading other software onto the laptop? |
| Network Security | | |
| 84 | General | Are networks segregated physically and/or logically to separate systems containing personal information from public networks such as the Internet? |
| 85 | General | Where a local area network containing personal information is connected to a public network, does the organization use perimeter defence safeguards (e.g. firewalls, routers, intrusion detection or prevention systems, anti-virus/anti-spyware software, etc.) to mediate all traffic and to protect systems that are accessible from the Internet? |
| 86 | General | Are systems that are exposed to the Internet (e.g. web servers and their software) or servers supporting sensitive applications "hardened" (e.g. by removing or disabling unnecessary services and applications and properly configuring user authentication)? |
| 87 | General | Are ports closed or Internet connections disabled on computers where services are not needed? |

| # | Heading | Question |
|--------------------------|---------|--|
| 88 | General | Are these safeguards regularly updated? |
| 89 | General | Are expert websites and vendor software websites regularly checked for alerts about new vulnerabilities and patches? |
| 90 | General | Are SSL (Secure Socket Layer) or other secure connection technologies (e.g. virtual private network (VPN)) used when receiving or sending personal information? |
| Wireless | | |
| 91 | General | Is there a policy in place that addresses the use of wireless technology? |
| 92 | General | Does the organization ensure that wireless networks are not used until they comply with the organization's security policy? |
| 93 | General | Are users on the network aware of the risks associated with wireless technology? |
| 94 | General | Does the organization have a complete and current inventory of all wireless devices? |
| 95 | General | Does the organization perform comprehensive security assessments at regular and random intervals (including identifying, locating and removing unauthorized wireless access points and other devices)? |
| 96 | General | Has the organization completed a site survey to measure and establish the wireless coverage for the organization? |
| 97 | General | Are access points located in such a way as to minimize the risk of unauthorized physical access and manipulation? |
| 98 | General | Are access points located in the interior of the organization's premises instead of near external walls and windows? |
| 99 | General | Are default parameters on wireless devices (e.g. passwords, identification codes) changed? |
| 100 | General | Are the strongest available security features of the wireless devices, including encryption and authentication, enabled? |
| 101 | General | Are additional safeguards (e.g. firewalls, anti-virus, etc.) installed on all wireless devices? |
| 102 | General | Are wireless capabilities (e.g. wireless cards in laptops) disabled (either permanently or when not required)? |
| 103 | General | Are unnecessary services (e.g. file sharing) disabled? |
| 104 | General | Is a wireless intrusion detection and prevention capability deployed on the network to detect suspicious behaviour or unauthorized access and activity? |
| 105 | General | Are audit records of security- and privacy-relevant activities on the wireless network created and reviewed on a regular basis? |
| Database Security | | |
| 106 | General | Is a data dictionary (table of contents) used to document, standardize and control the naming and use of data? |
| 107 | General | Is access to the data dictionary restricted and monitored? |
| 108 | General | Are database maintenance utilities that bypass controls restricted and monitored? |
| 109 | General | If there is a software failure, is the system capable of automatically recovering the database? |
| 110 | General | Have automated or manual controls been implemented to protect against unauthorized disclosure of personal information? |
| 111 | General | Are methods in place to check and maintain the integrity of the data (e.g. consistency checks, checksums)? |
| 112 | General | Are expert websites and vendor software websites regularly checked for alerts about new vulnerabilities and patches? |

| # | Heading | Question |
|--------------------------------------|---------|--|
| 113 | General | Are there technical intrusion-detection and security-audit programs to identify and address any unauthorized attempts to access information? |
| 114 | General | Are default parameters on the database (e.g. accounts, passwords, etc.) changed? |
| 115 | General | Is there a formal approval process in place for handling requests for disclosure of database contents or for database access, and does this process include steps to evaluate privacy impacts and security risks? |
| Operating Systems | | |
| 116 | General | Are operating systems kept up-to-date with all patches and fixes? |
| 117 | General | Is there a regular schedule for updating definitions and running scans with anti-virus, anti-spyware and anti-rootkit software? |
| 118 | General | Are expert websites and vendor software websites regularly checked for alerts about new vulnerabilities and patches? |
| 119 | General | Are all network services (e.g. websites or e-mail servers) running on computers connected to the network documented and authorized? |
| 120 | General | Are there technical intrusion-detection and security-audit programs to identify and address any unauthorized attempts to access information? |
| 121 | General | Is accurate time and date information maintained on computers to track malicious usage or errors appropriately? |
| Email and Fax Security | | |
| 122 | General | An organization should consider whether it is appropriate to transmit personal information by e-mail or fax. If it decides to do so, is a policy in place that addresses the use of fax and e-mail transmission of personal information? |
| 123 | General | Are regularly updated lists of fax numbers, e-mail addresses and other contact information produced and distributed to ensure that employees use current and accurate contact information? |
| 124 | General | If using a stand-alone fax, are the following steps taken when communicating PHI?: - the receiver is notified in advance of the fax? - the receiver stands by to receive the data or the receiver confirms that their fax machine is in a secure location? - a cover sheet is always used that contains a privacy notice with contact information? - frequently used numbers are programmed? |
| 125 | General | Are fax machines used to send or receive personal information positioned in a secure area? |
| 126 | General | Is access to fax machines used to send and receive personal information controlled using access keys and passwords? If faxes are stored on the network, is access to the folder restricted? |
| 127 | General | Are fax activity history reports retained to check for unauthorized transmissions? |
| 128 | General | Are fax machines used for the transmission and receipt of personal information only used by authorized staff? |
| Data Integrity and Protection | | |
| 129 | General | Is there a procedure in place to ensure that any removal of personal information from the premises has been properly authorized? |
| 130 | General | Is there an archiving process that ensures the secure storage of data, and guarantees the continued confidentiality, integrity and availability of the data? |
| 131 | General | Are encryption and other secure mechanisms in place for both the transport and storage of personal information? |

| # | Heading | Question |
|-----------------------|--|---|
| 132 | General | Are automated or manual controls, or both, used to prevent unauthorized copying, transmission, or printing of personal information? |
| 133 | General | Are there policies and procedures in place to protect against unauthorized modification of data? |
| 134 | General | When transmitting personal information where data integrity is a concern, is an integrity mechanism used to verify that the data has not been altered during transmission (e.g. digital signatures)? |
| 135 | General | Is there a process to revert and resolve changes if the data-integrity verification process fails? |
| 136 | General | Are data and software integrity tools used to detect unexpected changes to files? |
| Access Control | | |
| 137 | General | Is there an access control policy? For example, are there policies requiring username and password when you log in? Are there policies governing access to the operating system and each database? |
| 138 | General | Does the network access policy include a requirement that each user, at login, is informed of the date and time of the last valid logon and any subsequent failed logon attempts? |
| 139 | General | Are controls in place to detect any discrepancies in logon attempts? |
| 140 | User Registration, Access and Approval | Is a formal user registration process in place? |
| 141 | User Registration, Access and Approval | Does the user registration process include: verification of access levels, maintenance of records of access privileges, audit processes, and actions to ensure access is not granted until formally approved? |
| 142 | User Registration, Access and Approval | Is each user of a system that processes personal information uniquely identified? |
| 143 | User Registration, Access and Approval | When assigning a unique identifier for users, does the organization ensure the proper identification of the individual to whom the identifier is being issued, before giving the user access to the system? |
| 144 | User Registration, Access and Approval | Is the identification of the authorizer retained in the transaction record? |
| 145 | User Registration, Access and Approval | Is a current, accurate inventory of computer accounts maintained and is it reviewed on a regular basis to identify dormant, fictitious or unused accounts? |
| 146 | Roles | Is there a formal process to assign defined roles to users? |
| 147 | Roles | Does the access control policy clearly state the information access privileges for each defined role in the organization? |
| 148 | Roles | Does the role assignment process contain steps to ensure personal information is withheld from unauthorized individuals (e.g. manufacturers, maintenance staff)? |
| 149 | Roles | Is a data custodian role defined that includes access control, data integrity, as well as backup and recovery? |
| 150 | Roles | Has the role been defined for maintaining the access control lists? |
| 151 | Roles | Are roles and access rights for partners and third-party organizations (such as consultants, off-site storage) clearly defined? |
| 152 | Roles | Are privileges allocated on a need-to-use basis, and allocated, modified or changed only after formal authorization? |
| 153 | Roles | Are access privileges limited to the least amount of personal information required to carry out job-related functions? |
| 154 | Roles | Is there a clearly defined separation or segregation of duties (e.g. someone who initiates an event cannot authorize it; roles cannot overlap)? |

| # | Heading | Question |
|---|----------------|--|
| 155 | Roles | Is a monitoring process in place to oversee, manage and review user access rights and roles at regular intervals? |
| 156 | Authentication | Where a system user is authenticated, is the authentication information, such as password, not displayed, and is it protected from unauthorized access? |
| 157 | Authentication | Where user identification and authentication mechanisms are used to protect personal information, are procedures implemented that control the issue, change, cancellation and audit of user identifiers and authentication mechanisms? |
| 158 | Authentication | Where user identification and authentication mechanisms are used to protect personal information, are procedures implemented that ensure that authentication codes or passwords are generated, controlled and distributed so as to maintain the confidentiality and availability of the authentication code? |
| 159 | Authentication | Are the authentication mechanisms that are implemented commensurate with the sensitivity of the information and the associated risks (i.e. the more sensitive the information, the more robust the authentication mechanisms. For example, is two-factor authentication used when handling sensitive personal information, including financial information)? |
| 160 | Authentication | Where authentication is based on username and password, are effective password policies in place? |
| 161 | Authentication | Are passwords known only to the authorized user of the account? |
| 162 | Authentication | Are passwords pseudo-random in nature or vetted through a verification technique designed to counter triviality and repetition? |
| 163 | Authentication | Are passwords no less than eight characters in length? |
| 164 | Authentication | Are passwords one-way encrypted? |
| 165 | Authentication | Are passwords excluded from unprotected, automatic logon processes? |
| 166 | Authentication | Are passwords changed at least semi-annually? |
| 167 | Authentication | Are passwords changed at frequent and irregular intervals? |
| Information Systems Acquisition, Development and Maintenance | | |
| 168 | Hardware | Are security requirements identified as part of any new system development, acquisition or enhancement? |
| 169 | Hardware | Does the organization have a configuration-management or change- control process (e.g. source code control, tickets and resolutions)? |
| 170 | Software | Are privacy and security considered in the process of obtaining new third-party software? |
| 171 | Software | Is there a patch management process for new security vulnerabilities? |
| 172 | Software | Is there a separate environment for development and testing? |
| 173 | Software | Do the development and testing environments contain test data only? Test data should not be drawn from current or past real data. |
| 174 | Software | Are development personnel restricted from having access to the production environment? |
| 175 | Software | Is there a policy that prohibits the use of unauthorized software? |
| 176 | Software | Are there controls that prevent or detect unauthorized software? |
| 177 | Maintenance | Are systems containing personal information maintained only by appropriately screened personnel? |
| Incident Management | | |
| 178 | General | Is there a privacy incident management policy in place? Has the organization appointed an individual or established a centre to coordinate incident response? |

| # | Heading | Question |
|-------------------------------------|---------|---|
| 179 | General | Is there a privacy incident management policy in place? Do these procedures include guidance for the exchange of incident-related information with designated individuals and organizations in a timely fashion? |
| 180 | General | Does the privacy incident management policy include incident detection and analysis? |
| 181 | General | Does the privacy incident management policy include containment, mitigation and recovery strategies? |
| 182 | General | Does the privacy incident management policy include notification and reporting requirements? |
| 183 | General | Does the privacy incident management policy include post-incident analysis ("lessons learned")? |
| 184 | General | Does the privacy incident management policy include prevention strategies? |
| 185 | General | Are the individuals assigned to incident response roles adequately trained? |
| 186 | General | Are the incident response procedures practised and tested on a regular basis? |
| 187 | General | Does the organization use a variety of mechanisms (e.g. firewalls, routers, intrusion detection and prevention systems, audit logs, system performance tools, etc.) to continuously monitor the operations of their systems to detect anomalies in service delivery levels? |
| 188 | General | Does the organization maintain records that show how incidents were handled? |
| 189 | General | Does the organization perform a post-incident analysis that summarizes the cause and impact of the incident, and identifies security deficiencies? |
| Business Continuity Planning | | |
| 190 | General | Is there a process in place to develop and maintain business continuity throughout the organization? |
| 191 | General | Has the organization conducted an impact analysis to identify and prioritize the organization's critical services and assets? |
| 192 | General | Does the business continuity plan address different levels of interruption of service? |
| 193 | General | Does the business continuity plan address physical damage? |
| 194 | General | Does the business continuity plan address environmental damage? |
| 195 | General | Does the business continuity plan address unauthorized modification or disclosure of information? |
| 196 | General | Does the business continuity plan address loss of control of system integrity? |
| 197 | General | Does the business continuity plan address physical theft? |
| 198 | General | Has the organization made provisions for the continuous review, testing and audit of business continuity plans? |
| 199 | General | Has the business continuity plan been subject to appropriate departmental or regulatory expert review (e.g. legal, policy, finance, communications, information management and human resource specialists)? |
| 200 | General | Are backup processes in place to protect essential business information such as production servers, critical network components, configuration backup, etc? |
| 201 | General | Are backups stored offsite? |
| 202 | General | Are remote backups and recovery procedures tested at regular intervals? |
| 203 | General | Where 100% availability is essential, are duplicate databases maintained on separate physical devices and are all transactions performed simultaneously on both databases? |
| 204 | General | Have all databases and data repositories been identified? |
| 205 | General | Are mechanisms in place to monitor the organization's level of overall readiness? |
| Compliance | | |

| # | Heading | Question |
|-----|----------------------|---|
| 206 | Audit Process Design | Are all relevant statutory, regulatory and contractual requirements explicitly defined and documented for each information system? |
| 207 | Audit Process Design | Are all system/audit logs that relate to the handling of personal information: Securely and remotely logged to a read-only medium that has an alert system when tampering is attempted? |
| 208 | Audit Process Design | Are all system/audit logs that relate to the handling of personal information: Regularly monitored? |
| 209 | Ongoing Audits | Are procedures in place to ensure that security events (e.g. unauthorized access, unsuccessful system access attempts, etc.) are identified, recorded, reviewed and responded to promptly? |
| 210 | Ongoing Audits | Are proactive audits conducted at regular intervals to verify the logical and physical consistency of the data, in order to identify discrepancies such as lost records, open chains, incomplete sets and improper usage? |
| 211 | Ongoing Audits | Is active monitoring in place to ensure that personal information cannot be passed between computers, or between discrete systems within the same computer, without authority? |
| 212 | Scheduled Audits | Is software/hardware inventory maintained in an up-to-date fashion? |
| 213 | Scheduled Audits | Is an annual physical inventory of all storage media containing personal information performed and are discrepancies investigated immediately and corrected? |
| 214 | Audit Verification | Are audit monitoring and review procedures in place to promptly detect errors in procedures and results? |
| 215 | Audit Implementation | Do the management personnel responsible for the audited area oversee the implementation of audit recommendations, verify completion of implementation and report verification results? |

End

Created on: 04-Jul-2017
Last Updated on: 24-Sep-2017