PRIVACY IMPACT ASSESSMENT GUIDELINES

Ministry of Justice
Access and Privacy Branch

Telephone: (306) 798-0222
Email: accessprivacyjustice@gov.sk.ca

April 2017

Government of Saskatchewan

Table of Contents

AN OVERVIEW: PRIVACY IMPACT ASSESSMENTS

What is a Privacy Impact Assessment (PIA)?

Privacy Impact Assessments (PIAs) are a tool used to identify and evaluate privacy risks and their impacts and help mitigate or reduce them to an acceptable level. PIAs take a close look at how government agencies protect **personal information** and/or **personal health information**[1] (hereafter referred to as "personal information") as it is collected, used, disclosed, stored and ultimately disposed of.

PIAs promote compliance with the privacy protection responsibilities under *The Freedom of Information and Protection of Privacy Act* (FOIP) and *The Health Information Protection Act* (HIPA). They promote transparency and accountability, and contribute to continued public confidence in the way government manages personal information.

When is a PIA required?

At present, there is no legislative requirement for the completion of PIAs in Saskatchewan.

Though not statutorily required, PIAs are a privacy best practice; they are also part of good information governance and a good business practice. They are a means of addressing project risk as part of overall project management - just like conducting a security review or needs assessment is an important part of many projects.

Government institutions should consider a PIA any time it creates, modifies or reviews a program or activity that involves personal information. A PIA will help ensure the program is compliant with the law and that obligations to protect privacy have been met.

A PIA should be considered when:

- a project, program or application is new and privacy impacts have not been examined in detail before;
- an existing project, program or application undergoes a change or redesign such as:
    - expanding the number of partners involved;
    - adding to or changing the collection, use, disclosure and disposition of personal information;
    - changing technical aspects of how the data will be managed, accessed, etc.;

[1] The definitions of personal information and personal health information are found in *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act.*

- privacy implications have not been considered in the past and/or no legal review has been done;
- the project involves one or more partners;
- the personal information involved in the project is particularly sensitive (the Government of Saskatchewan's *Guide for Information Protection Classification* may be helpful when considering the sensitivity of personal information); or
- the project is high profile and will likely draw interest from the public.

Whenever personal information is involved in a project, government institutions must be satisfied that legal obligations for the protection of privacy have been met. It is highly recommended that the project sponsor consult with the government institution's legal counsel and Privacy Officer.

Carrying out preliminary privacy analysis (attached as Appendix A) is a good way to assess the privacy implications of a project. If a decision is made to not undertake a PIA based on this analysis, a record of that decision and the supporting rationale should be retained. If a full PIA is undertaken, the work undertaken in the preliminary analysis can be used.

PIAs can be completed at any stage; however, completing a PIA during the planning stage - before a new program or service begins - is the best way to ensure the privacy risks are fully understood. Periodic updates to ensure the original PIA reflects the current situation are also recommended.

What does a PIA consider?

Among other things, a PIA will consider the following aspects of a project:

Accountability/Governance – for example:

- Have you decided who is responsible for various aspects of the program, including privacy? Is the governance understood by all involved? Who makes decisions about access and disclosure?

Collection, Use and Disclosure – for example:

- Do you have authority to collect the personal information? Do you collect only what is necessary for the purpose?
- Do you have authority to use and disclose the information for the intended purpose? Will consent be required or collected?
- Have you taken steps to inform individuals of the purpose for collection?

Accuracy and Retention – for example:

- How are questions regarding information accuracy addressed?
- Is there a retention schedule that applies to the personal information?
- Is personal information in all forms retained only as long as necessary?

Safeguards – for example:

- Has a security review been conducted?
- What safeguards are in place?
- Are staff trained in appropriate collection, use and disclosure?

Access Rights – for example:

- Do you have a method in place to allow individuals to access their personal information?
- Can records be amended?
- Is there a process to handle public questions or concerns?

PIA Timelines

All projects are different and so are their PIAs. If a project involves multiple government institutions and components, it may require a complex PIA or more than one PIA that may take several weeks or months to complete. Alternatively, if the PIA is for a simpler project, such as one collecting survey data, it may only take a few days to complete.

In order to avoid delays in project development and implementation, it is important to begin a PIA at the earliest stages of the development of a project, when it is still possible to influence project design from a privacy perspective. Generally speaking, the best stage to do a PIA is after all business requirements and major features of the project have been determined in principle, but before completing detailed design or development work to implement those requirements and features.[2]

[2] Office of the Information and Privacy Commissioner (OIPC) of Alberta, Privacy Impact Assessment (PIA) Requirements, for use with the Health Information Act, January 2009, which can be found at www.OIPC.ab.ca p.13.

GETTING STARTED – PART 1 OF THE PIA

Before You Start - Preliminary Analysis and Project Planning

The first step is to determine - through preliminary analysis of the type of information involved in the project - if a PIA needs to be conducted. Preliminary analysis should be conducted as early as possible in the project so that the resulting PIA process can be considered in ongoing project planning.

To carry out your preliminary analysis, among other things, you should gather:

- any relevant/previous PIAs already completed around this project;
- any legislation (other than FOIP and HIPA) that is relevant to the project;
- any relevant business documents such as the Project Charter (which describes what the nature of the project, how it will be approached and lists all partners and stakeholders);
- information about data involved in the project (where it is stored, how it is accessed, how access is controlled, where the data flows, etc.);
- any records retention schedules for the project;
- any relevant agreements (Information Sharing Agreements, Memorandums of Understanding, Research Agreements, etc.); and
- information about any processes required to obtain approval from program managers and executive leadership.

With the information you have gathered, you can begin to determine if a PIA is needed.

Start by creating a list of all the elements of information and data included in your project. This includes, but should not be limited to, personal information. This catalogue of information can then be assessed against privacy legislation to determine if it is covered by those laws and helps to set the foundation for the remainder of the PIA review.

You should then write a description of the system, project, program or activity that would be the subject of the PIA. Whether you are building a new system for your government institution or setting up a new social media page, you will want to give as much relevant detail as possible about your project.

When you write the description, assume the reader is not familiar with the project or any of the relevant background information. Write in plain language, avoid jargon or abbreviations and be as precise, clear and concise as possible. It is often helpful to answer the "who, what, where, when, why and how" questions about a project when contextualizing it:

- What is the project and its purpose? - This section should clearly articulate the purpose of the project. It should answer the questions "Why are we doing this project?" and "What are the benefits of the project?" It should also describe the project. Is it a new

service for existing clients, an effort to improve services or a way to streamline government processes?
- Who is involved in this project? - Is it one government institution or a shared service project amongst multiple government institutions? Does it involve federal government or private sector partners?
- Where is the project taking place? - Is it online, in person or paper-based?
- When is the project occurring? - Is it a revision to an ongoing project or a new one that will begin in six months?
- Why is the project happening? - Does it fulfill a legislative requirement? Is it an effort to meet demands for online service delivery? Is it to improve an existing service or activity?
- How is the project being implemented? – Will it be a phased implementation or will it be rolled out in complete form?

Based on the above, and in consultation with your Privacy Officer, you will need to determine if a PIA is warranted. If it is determined that a PIA is not necessary, the decision not to proceed and how it was reached and approved should be documented and retained.

When a decision is made to conduct a PIA, planning must be undertaken to determine the scope of the PIA, resources required and projected timelines.

Assemble a Team

A team will need to be assembled to complete the PIA. The size and membership of the team will vary based on the complexity of the PIA; often, it will include subject matter experts with knowledge in the following areas:

- Privacy: issues, policies, practices, principles and applicable legislation;
- Information Technology: relevant technology policies, practices and standards;
- Security: relevant physical, technical and procedural security safeguards;
- Information Management: relevant policies, practices and standards;
- Records Management: retention, archives, and disposal of records;
- Legal: applicable privacy legislation, enabling legislation, bylaws and other legal requirements, service level agreements, memoranda of understanding, contracts, etc.;
- Risk Assessment: risk assessment methodology;
- Procurement: acquired or outsourced product and service solutions;
- Business Processes: relevant business processes, roles, responsibilities and resources; and
- End-Users: staff who will use the system can speak to practical implications.

A PIA lead should be identified. It may be helpful to develop a work plan for the PIA during this step.

Define Scope

Team members should define and agree upon the scope of the PIA. The scope of the PIA should have approval from the project lead and other relevant decision-makers. In determining the scope of a PIA, many factors will need to be considered, such as whether:

- the privacy risks and impact apply to all or to only some parts of the project;
- the PIA will cover all associated business processes and technology;
- any components of the project have already been considered in other PIAs;
- the PIA covers a specific change to an existing program, process or system, but not the entire system; and
- another area is responsible to analyze specific parts of a joint project.

SOME OTHER PRELIMINARY CONSIDERATIONS

Records Management

Where, how and for how long personal information is stored, who has access to it and how it is accessed, and when and how the personal information will be destroyed, are important details to consider in your preliminary analysis. Important details, such as if personal information will be stored outside of the province or if cloud storage is being considered, should be included in your preliminary analysis. It is also important to consider where the people who will have access to project data are located. Are all technical support professionals within Canada? Will staff be able to remotely access personal information?

Common Integrated Services

If your project is a program or activity designed to benefit the health, safety, welfare or social well-being of an individual and is delivered by a government institution and certain other partners, it may be considered a "common or integrated service" under section 17.1 of *The Freedom of Information and Protection of Privacy Regulations* and section 5.2 of *The Health Information Protection Regulations*. In these circumstances, you will need to have specific documentation in place to meet regulatory requirements. This should be specifically noted in your preliminary analysis.

Data Linking

Some projects may seek to use personal information or de-identified data from different databases in order to conduct research, assessment or analysis. This is an important consideration as, often, the purpose for which the information in each database was originally obtained or compiled will not be consistent with how it is proposed to be used in the project.

It is also important to consider situations where data is being linked between two or more government institutions or between a government institution and another agency.

Where de-identified or non-nominal information is being used, it is still important to consider the potential impacts of data linkage and the possibility of re-identification and/or the possibility of creating new personal information through the compilation of other information.

PROJECT ANALYSIS – PART 2 OF THE PIA

In order to effectively assess the privacy impacts of a project, you will need to have a full understanding of the project under consideration. This requires you to compile the information needed to carry out a detailed privacy analysis. A completed project analysis will identify, among other things:

- how personal information will be collected, used, disclosed, retained, secured and disposed of;
- the authorities for each activity;
- who is responsible for the personal information and how;
- what technology will be used for each of these activities;
- personal information access privileges and the purpose for the privileges; and
- how personal information flows.

To complete project analysis gather:

Background Information

- All project-related documentation, including information about business processes, workflow, information flows and business rules; where possible use existing documentation such as the project's business case, Memorandums of Understanding, agreements, and other project management documentation, previous privacy and security assessments, training materials, policies and procedures and business and IT design documents.

Relevant Business Processes

- All relevant business processes should be documented in a general way.
    - Business processes can include anything from technical processes (such as system back-ups or data processing), to administrative functions (such as reviewing applications, filing and archiving), to policy and ongoing monitoring of the program, system or process.

Possession/Custody or Control

- The analysis should consider who has possession or control of the information. The term "possession" is used to describe the physical location of the

information. Whereas "control" is determined by a government institution's authority to manage, regulate and administer the use, disclosure or disposition of the information. A government institution may not have physical possession of a document but may have control of it. A record is under the "control" of a government institution if the contents of the document are related to a departmental matter and if the government institution reasonably expects to obtain a copy of the document upon request[3]. Information is in the possession of a government institution if it has physical possession plus a measure of control of the information[4].

- It is important to consider the ongoing responsibilities of government institutions when services are delivered through contractors or provided by Information Management Service Providers (IMSPs);
- Contracts and information sharing agreements should be in place and should consider the legal authority and the way information will be managed throughout the service;
- Where a contractor or IMSP provides services for or on behalf of a government institution, information involved in those services may be under the control of the government institution unless contracts or agreements provide otherwise.

Roles and Responsibilities

- The roles and responsibilities of all those involved in the project – including partners and third parties - should be identified and documented. Particular attention should be paid to those persons or positions which may access or manage personal information.

Personal Information Flows

- Determine the various types of information that will be collected, accessed, used, retained, disclosed, secured or disposed of during each business process and activity; particular attention must be paid to personal information.
- Determine how the personal information involved in this project will flow through the business processes and technology from collection to final disposition.

Supporting Technology

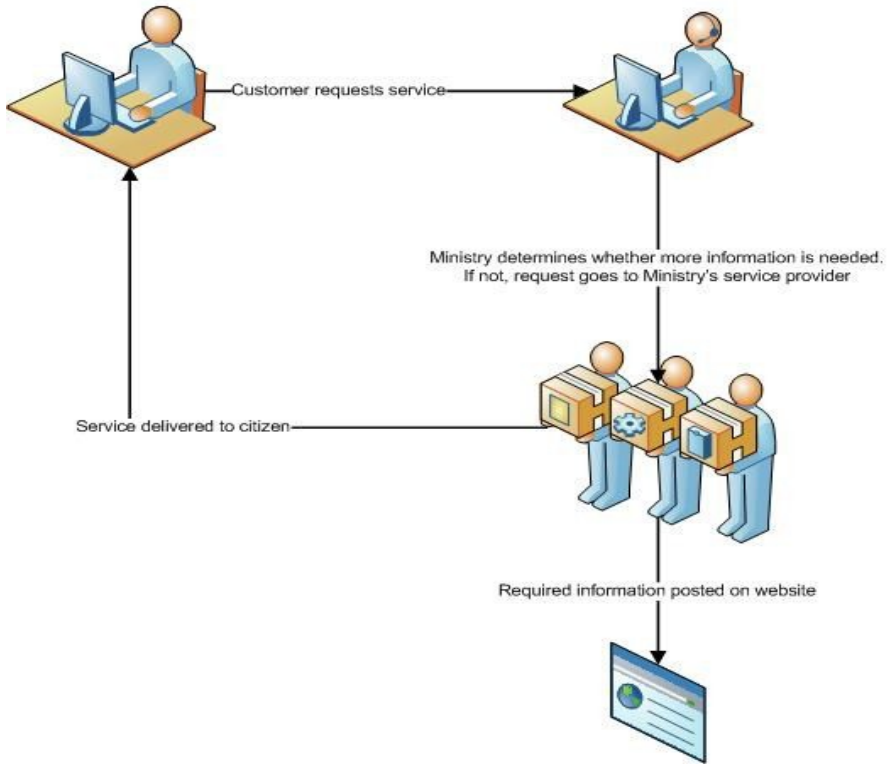
- Identify and document the technology-related components of the project. Consider if technology being used or developed by the project has privacy implications by determining, among other things, how the technology interacts with personal information and who will have access to personal information used in each technology.

[3] Canada (Information Commissioner) v Canada (Minister of National Defence), 2011 SCC 25
[4] *IPC Guide to Exemptions for FOIP and LAFOIP at page 73*

PERSONAL INFORMATION FLOWS

Verbal descriptions of information flows are helpful, but visual representations are often an easier way to demonstrate and understand how personal information flows in a project. A flow diagram, accompanied by a table that cites the relevant authorities, is one of the most effective ways of showing how your project will collect, use, disclose and/or dispose of personal information.

Figure 1 – Flow Diagram and Table



SAMPLE PERSONAL INFORMATION FLOW TABLE				
	Description/Purpose	**Personal Information Involved**	**Type**	**Authority**
1.	Email service request from client	Name, services used/needed	Collection	FOIP 25
2.	Email to client seeking more information	Name, issue description	Use	FOIP 28(a)
3.	Service request provided to another Ministry to deliver services	Name, services used/needed	Disclosure	FOIP Regulations 29(2)(a)

The key to an effective information flow table is to break down your project into its most basic parts. Explain information flows simply, so that a person unfamiliar with the project can understand it as easily as a person who is familiar with the project.

Special attention should be paid to the process points where:

- personal information is collected from someone/somewhere;
- there are uses of personal information;
- personal information is disclosed or shared; and
- personal information is disposed of.

At each of these stages, the data minimization principle should be considered so that no more personal information than is required is collected, used, disclosed and ultimately stored. It is important to also remember that authority must exist for the collection, use, disclosure or disposal of personal information.

Whether information is collected directly from an individual or is gathered from another source, the authority for the collection should be established before the collection occurs. Generally, the authority to collect personal information can be found in FOIP and HIPA. For some government institutions, the authority to collect personal information may exist in their enabling legislation or other acts. Every instance in which personal information is collected should have the authority for the collection documented.

Collection of Personal Information

Personal information can be collected from a variety of sources. It is important to remember that personal information must be collected from the individual to whom it relates unless there is authority in s. 26 of FOIP or s. 25 of HIPA for indirect collection. It is also important to consider the definitions of personal information and personal health information found respectively in FOIP and HIPA when determining what kind of information you collect and where the information comes from. Examples of potential personal information collection sources include:

- Application or submission forms;
- Comment boxes or web postings;
- Consultations and surveys;
- Correspondence; or
- Receiving personal information about an individual from another program area within your government institution, or from another government institution or organization

Your information flow table should also describe when your project uses personal information that has been collected or is already in your possession or control. A use occurs when personal information is used within the program areas of your government institution. It is important to remember that the use of personal information requires the consent of the

subject individual or authorization under the acts. Your table should document each use and the specific authority that allows the use.

The same steps should be taken with any disclosures of personal information involved in your project. You should document all instances in which personal information is disclosed or shared outside of your organization and the authority for the disclosure.

Disclosure of Personal Information

There are legal authorities under FOIP and HIPA under which personal information may be disclosed. It is important to identify the nature of the disclosure and the authority under which it occurs. Examples of potential personal information disclosures include:

- Transferring information to or sharing information with another government institution or organization;
- Publishing information in print or online (or allowing people to post publicly to your website);
- Verifying information for another government institution or organization; and
- Providing information upon request (e.g. from police, citizens, a ministry, etc.).

It is important to identify the nature of the disclosure and the authority under which it occurs. Disclosure occurs when personal information is released, transmitted, revealed or otherwise exposed outside of a government institution to a separate entity that is not a part of the government institution, or to a person or persons who are not employees of the government institution.[5]

Unless you obtain the consent of the individual whose personal information is being disclosed, a legal authority for disclosure is required. The authorities for disclosure without consent under FOIP and HIPA have specific applications; your privacy branch and legal counsel should be consulted when determining the appropriate authority for disclosing personal information without consent.

Finally, your information flow table should also describe when and how the personal information involved in your project will be retained or disposed of. You should note relevant retention and destruction schedules and include information about retention and destruction methods used in your project. Your records management branch should be consulted to ensure compliance with *The Archives and Public Records Management Act*

[5] SK OIPC INVESTIGATION REPORT 219-2015 p.3

PRIVACY ANALYSIS – PART 3 OF THE PIA

Whenever a government institution collects, uses, discloses, stores or disposes of personal information, it must take reasonable steps to protect that personal information. In this step, privacy risks and impacts are identified and analyzed. Proposed solutions addressing the privacy risks are detailed and examined.

A privacy impact is any negative outcome on identifiable individuals, groups, organizations or institutions that is the result of an unmitigated privacy risk. An example of a privacy impact can be found in unauthorized accesses of personal information, such as snooping. Instances of snooping create a privacy impact that leads to individual concerns around the confidentiality and security of information and threats such as stalking or harassment. On an institutional level, snooping creates potential privacy impacts in legal risk, reputational damage and a loss of public trust.

Privacy Impacts

A privacy impact is anything that could adversely affect the privacy of personal information. Examples of privacy impacts are numerous and can be found in circumstances such as:

- insufficient legal authority to collect, use or disclose personal information;
- utilizing inaccurate or outdated information;
- retaining personal information for longer than it is needed or required, or disposing of personal information when retention is required;
- lack of appropriate safeguards; or
- lack of processes for individuals to access and request correction to their personal information.

To carry out your privacy analysis you will:

IDENTIFY POTENTIAL PRIVACY IMPACTS/RISKS

When gaps in existing and planned privacy protection measures do not address privacy, there is a potential privacy risk. Essentially, a privacy risk is anything that falls outside of the mantra "right information, right person, right purpose, right time, right way." The privacy impact is the end result that may occur if a privacy risk is not mitigated.

The Preliminary Privacy Analysis Worksheet (Appendix A) can be used to identify potential privacy risks and impacts and test the project against identified privacy requirements. Input from the various subject matter experts you have pulled together as part of your PIA team should be relied upon to assist with the identification and analysis of privacy impacts. Once complete, the checklist will help form the basis of the privacy analysis and should be included in the PIA report (Step 4).

ANALYZE FINDINGS

Every project that collects, uses or discloses personal information has some degree of privacy risk. These risks must be assessed against a number of factors including:

- the likelihood of the risk occurring;
- operational considerations such as the resources associated with addressing the privacy impact; and
- the impact of the risk should it occur, including factors such as:
    - the scale of impact;
    - the nature of the impact of those affected; and
    - the potential impact on institutional reputation and in public confidence.

The tables found in Appendices C and D can be used in assessing the likelihood and potential impacts of a privacy risk.

The analysis of privacy impacts and development of mitigation strategies should consider business requirements while ensuring legislative compliance and providing appropriate levels of privacy protection.

IDENTIFY PRIVACY SOLUTIONS

For each privacy risk, possible solutions or actions that will mitigate the risk should be identified. Compliance with access and privacy legislation requires that reasonable steps are taken to establish and implement privacy protection measures to protect personal information.

The measures suggested to address specific privacy risks and the anticipated effectiveness of those measures should be described in detail, including whether the solution will eliminate the risk or reduce it a level that is acceptable to project managers. This will include any administrative, technical or physical safeguards intended to address the privacy risk and protect:

- the integrity, accuracy and confidentiality of the information;
- against any reasonably anticipated threat, hazard or loss of the information; and/or
- from unauthorized access to or use, disclosure or modification of the information.

When detailing safeguards, ensure you describe any and all security measures that are or will be in place. This may be technical security (such as passwords and firewalls), physical measures (such as locked cabinets and secure physical sign-in to buildings) or administrative safeguards (such as policy manuals and training programs). Make specific note of any

existing systems that track who has accessed information, when it was accessed, for how long and what uses of or changes to the information have been made.

You should cite the policies and procedures being used for the protection of information. This may include organizational policies (e.g. your organization may restrict access to personal information to only those employees who need the information in order to carry out their roles and responsibilities) or policies developed specifically for certain branches or work-units (e.g. employees in your branch may not be permitted to access certain data remotely).

For each risk identified, you should also estimate the likelihood of the risk occurring and what the impact would be if it occurred. The analysis of proposed solutions, including the likelihood and impact of risk, should allow project managers to select the solutions that will provide the greatest benefit to the project and those affected by it.

Make sure that you consider the privacy solutions that may already exist in your project. It is important that privacy sensitive practices and technologies that are part of the project be noted. You should, for instance, document your collection notification details. The acts require that the individual from whom personal information is being collected be provided specific information about the collection. If you have already developed a collection notification, you should ensure this is noted as a solution to a potential impact.

IDENTIFY ACTION ITEMS

A strategy to mitigate and manage the privacy risks of the project should be created based on the identified solutions. This strategy should include a list of items that must be carried out to ensure that the project protects privacy and is compliant with the Acts. This list should identify the parties responsible for implementing the solutions and monitoring the privacy impact.

OTHER CONSIDERATIONS

Accuracy, Correction and Retention of Personal Information

The Acts require that the personal information government institutions collect and use is accurate and complete. They also provide individuals with rights of access and a right to request a correction to their personal information if they believe it is wrong or incomplete.

Government institutions have certain obligations where a request for correction has been made.[6]

[6] Reference Section 32 of FOIP, section 31 of LA FOIP and section 13 of HIPA

Your PIA should include a list of the measures you will take to ensure the accuracy and completeness of personal information involved in your project. This could include error-proofing of forms, manually verifying information before decisions are made or periodic checks of databases.

Your PIA should consider and identify the steps your government institution will take to facilitate individual access to personal information involved with your project and how requests for correction will be handled. You should be able to answer questions such as:

- How will access to personal information be provided?
- Will individuals be able request a correction to their personal information?
- How will you make corrections to inaccurate personal information?
- Will incorrect information be clearly marked and/or removed and the correct information attached to the file?
- If a request for correction of personal information will not be made, how will this be noted?
- What steps will be taken to notify other holders of the personal information of the correction/annotation?

Privacy Breach Management

A PIA is a way to help identify and mitigate privacy risks; it will not prevent all privacy incidents, such as a breach of privacy, from happening. Your PIA should consider how privacy incidents will be handled, including how privacy breaches will be investigated and reported. Consult your Privacy Officer for the related policies for your government institution; further guidance can be found in the Privacy Breach Management Guidelines.

Information Sharing and Research

Your PIA should note if your project shares personal information with other government institutions or partners from outside provincial government. The PIA should explain from whom or to whom the personal information is being collected or disclosed and the purpose of and authority for collection and disclosure. In these cases, you should have prepared an Information Sharing Agreement for your project.

If your project is going to disclose personal information to researchers for research purposes, your PIA must record whether consent was obtained and, if not, why it was not reasonably practicable to do so, establish the authority for disclosure and describe why de-identified information could not be used. Make sure you include relevant information such as required agreements and research ethics committee approval, as well as approvals from external research ethics boards.

Risk Mitigation Table

A risk mitigation table is a useful visual reference that helps identify potential privacy risks that your project may have and how you intend to manage, mitigate or eliminate them. The table should list a project's risks (something that could cause unauthorized collection, use or disclosure of personal information), along with a corresponding likelihood, impact and mitigation strategy.

An example of a risk mitigation table is provided below:

RISK MITIGATION TABLE				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Employees could access and disclose personal information without authority.	Oath of Confidentiality; Role based information access; Privacy Policies; Privacy Training.	Low	High
2.	Service request may not be from client (i.e. concern that someone other than client may be asking for the service without the client's consent or approval).	Implement identification verification procedures.	Low	High
3.	Client personal information may be compromised when transferred to another Ministry.	Only use secure servers and encrypt transmissions.	Low	High
4.	Inherent risk of sending personal information to client via email.	Implement policy to advise clients of risk, offer alternative method of providing information and gather consent from client.	Medium	Medium

THE REPORT – PART 4 OF THE PIA

Preparing the Report

The results of the project and privacy impact analysis should be documented in a way that serves the purpose of the project and supports decision-makers. It will provide decision-makers with specific recommendations on how to address privacy impacts and enable them to make informed decisions about how the project should proceed.

The report template included in this package (Appendix B), or other preferred formats, should be used to complete a first draft of the PIA. Much of the information that will be contained in

the report may have already been completed or compiled during the preceding steps.

Prior to approval, a final review of the PIA should occur. The PIA should be reviewed for accuracy and provide all partners with an opportunity to ask questions and raise concerns. One of the key objectives of this exercise should be to ensure there are no surprises when the project "goes live."

At this stage, you may want to consider consultation with the Office of the Information and Privacy Commissioner (IPC). Alternatively, you may want to wait until all internal approvals have been completed before sharing with the Commissioner's Office. Either way, you should be prepared to receive and accommodate input from the IPC and revise the PIA as needed.

Information and Privacy Commissioner (IPC)

The IPC is an independent Officer of the Legislative Assembly mandated to oversee and ensure compliance with Saskatchewan's access and privacy legislation.

The IPC has the authority to comment on the implications for privacy protection of proposed government programs.

It is important to involve the IPC early on in the PIA process as it can provide guidance on how to bring your program into compliance. The IPC does not approve, endorse or sign off on your PIA.

You can learn more about the IPC at: www.oipc.sk.ca

After review, the PIA should be approved by the appropriate authority for the project. The PIA report should be approved and signed off in accordance with the institution's internal process. Typically, this review would include:

- The senior person for the program area (such as an Assistant Deputy Minister or Executive Director);
- The senior person in charge of information technology systems (such as an Assistant Deputy Minister or Executive Director)
- The Privacy Officer.

The review and approval processes ensure that the key players understand and support the analysis and any recommended actions included in the PIA.

Implementation

In order to address the risks identified by a PIA, the actions recommended in the PIA must be implemented.

As implementation of mitigation strategies progresses, privacy impacts should continue to be monitored and assessed; it may be necessary to update the PIA Report. In this way, the PIA process serves as part of an ongoing privacy risk identification and mitigation strategy and the PIA Report is an up-to-date record of that strategy. That strategy, including the PIA documentation, should be transferred to the appropriate parties, such as the program area, to enable ongoing privacy protection and the management of privacy risks once the program, process or system becomes operational. A copy of the completed and signed PIA should be retained in the program or business area and by the Privacy Officer.

WHO TO CONTACT FOR ASSISTANCE

If you have any questions regarding access, privacy or the PIA process, please contact the Access and Privacy Branch at:

- Email: AccessPrivacyJustice@gov.sk.ca
- Phone: (306) 798-0222

REFERENCES

- Office of the Saskatchewan Information and Privacy Commissioner PIA Guidelines: https://oipc.sk.ca/assets/privacy-impact-assessment-guidance-document.pdf
- Alberta PIA Guidelines: https://www.oipc.ab.ca/action-items/privacy-impact-assessments.aspx
- BC PIA Guidelines: http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments
- Ontario PIA Guidelines: https://www.ipc.on.ca/wp-content/uploads/2015/05/Planning-for-Success-PIA-Guide.pdf

APPENDIX A
PRELIMINARY PRIVACY ANALYSIS WORKSHEET GUIDE

A privacy impact assessment is an evaluative process which allows government institutions to assess, evaluate mitigate and, where possible, eliminate privacy risks associated with the collection, use, disclosure and retention of personal information and personal health information. As part of this process, preliminary privacy analysis is conducted to assist with completing a privacy impact assessment. This worksheet can be used and adapted by government institutions for this purpose. You may not need to answer every question, but please read through them and answer if applicable.

Where it is available, be sure to include all documentation as noted in this form. Please contact your Privacy Officer if clarification or assistance is required.

1. GENERAL INFORMATION	
Project Name	
Project Number	
Program Area Lead	
Phone Number	
Email	
Project Manager	
Phone Number	
Email	
Privacy Lead	
Phone Number	
Email	
Date Completed	

2. PROJECT OVERVIEW	
1	**Project Description** Provide a general overview of the project. If possible attach the ***Project Charter***, ***business requirements*** or other documentation. If a ***PIA*** has been previously completed for this project or a substantially similar project please attach. Identify any privacy risks.
	Among other things, the project description should answer the questions: • What is the purpose of the project? Why is it being undertaken? What business need is it fulfilling? • Why are you developing this new project or changing an existing one? (Is it required by policy or law? Is it fulfilling a specific mandate?) • Who is involved in the project? List all internal and external partners and participants. • What is the Governance Structure? Define the reporting structures and responsibilities associated with the initiative. • Who is responsible for the information involved in the project? o How are they responsible? o Who is in control of the data? o How are they in control? • Which individuals or groups will be consulted to assist with assessing and mitigating privacy risks related to this project? Describe the consultation process below. • When will the project start and end? Or, what is the project timeline? Privacy risks in this section include but are not limited to: • Project duration: o High risk projects retain data for more than three years and/or run for more than three years. o Low risk projects destroy data on the completion of the project and/or run for less than one year. • Data or project governance: o High risk projects involve four or more agencies and/or allow thirty or more personnel direct access to identifiable information. o Low risk projects involve only one agency and allow fewer than ten personnel direct access to identifiable information.

3. INFORMATION OVERVIEW	
1	**Information Description** Provide a general overview of the nature and type of information involved in the project, including in general terms how it will be collected, used, disclosed and/or retained. Include an ***Information/Data Flow Diagram*** where possible. Identify any privacy risks.
	Among other things, the information description should answer the questions: • What type of information is involved in the project? • Is personal information and/or personal health information involved in the project? If so, please describe that information. • To whom does the personal information relate? List all the data subjects/individuals whose personal information and/or personal health information will be involved in the project. • How will information be collected? • Who will use the information? • Will any information be disclosed? • Will any information be shared for common or integrated services? • Who will retain the information? Privacy risks in this section include but are not limited to: • Use of identifiable information: o High risk projects use identifiable information. Risk may increase depending on the nature and sensitivity of the information. o Low risk projects use de-identified information. Risk her should also be considered based on the nature of de-identification. For instance, the inclusion of a large number of quasi-identifiers in a de-identified data set increases privacy risk.

4. COLLECTION, USE, DISCLOSURE and/or RETENTION of PERSONAL and/or PERSONAL HEALTH INFORMATION	
1	**Information Collection** Section 25 of FOIP limits the collection of personal information by government institutions to information collected for the purpose of current or proposed programs or activities; in other words how the government institution will use or disclose the personal information. Section 23 of HIPA limits collection of personal health information to only what is reasonably necessary for the purpose. Section 26 of FOIP and sections 23-25 of HIPA describe how information may be collected. A government institution should be able to link the personal information and personal health information it collects to a legitimate business purpose; the collection should be limited to that which is reasonably necessary for the purposes identified by the government institution. It is a best practice for government institutions to collect, use and/or disclose the minimum amount of personal information and personal health information needed to accomplish the purpose(s) for which the information was collected, used or disclosed. Describe the way the project will collect information and the purposes for which information will be collected. Identify any privacy risks.

	Among other things, the description should answer the following questions:
	
	• What is the purpose for which the information is being collected?
	  o How does this relate to the purpose of the initiative?
	• Will the information be used for any other purpose?
	• Are all purposes authorized by legislation or regulations? If so, please identify the provision(s) of the relevant legislation.
	• Is the minimum amount of information being collected to satisfy the purpose for the collection?
	• Will the information be collected directly from the individual?
	• Will information be collected from other individuals or entities or from publicly available sources)?
	  o What specific legal authorities authorize indirect collection?
	• How often will the personal information be collected (once only or ongoing)?
	
	Privacy risks in this section include, but are not limited to:
	• Collection practices:
	  o High risk projects do not collect information from the subject but rely on various sources and do not confirm the accuracy of information.
	  o Low risk projects collect information from the subject or from limited sources which can verify the accuracy of information.

	• Data minimization: o High risk projects use more than the least amount of information necessary for the purpose of the project. o Low risk projects use the least amount of information necessary for the purpose of the project.

4. COLLECTION, USE, DISCLOSURE and/or RETENTION of PERSONAL and/or PERSONAL HEALTH INFORMATION	
2	**Notice** FOIP 26(2) requires government institutions to notify individuals from whom they are collecting personal information about the purpose of the collection. Please describe how individuals are going to be notified that their personal information and personal health information is being collected? Identify any privacy risks.
	Among other things, the description should answer the following questions: • Was any form of notice provided to the individual on how their information is to be collected, used and/or disclosed? If not, please explain why notice is not provided. • If so, how and when are individuals informed: in-person, by general notice, in a letter? • Are individuals provided with the name of someone who can answer questions about how their information will be collected? Privacy risks in this section include but are not limited to: • Notification practices: o High risk projects do not provide notice to subjects and/or provide notice in language that is unclear or confusing. o Low risk projects provide clear notice to subjects using plain language.

3	**Consent** Consent is the preferred option to provide the authority for government institutions to collect, use and disclose personal information and personal health information. Sections 26, 28 and 29 of FOIP set out the purposes or circumstances when personal information may be collected, used or disclosed without consent. HIPA 27(2) provides three ways to get consent from an individual: express consent, implied consent or deemed consent. Describe how consent will be sought from the individual? If consent is not being sought, please set out the legal authorities that authorize the collection, use and disclosure of the personal information or personal health information?
	Among other things, the description should answer the following questions: • Does the project seek consent of individuals whose information is being collected, used, and/or disclosed? If not, please explain why consent is not being sought and identify the provision(s) of the relevant legislation. • If the project seeks consent, how is informed consent obtained? In writing? Verbally? Why? o Is there a script, guideline, or a FAQ available? If so, please attach. o If applicable, is there legal authority for verbal consent? If so, what information must be documented? • Are there any limits to consent (i.e. is it possible for the person to consent to certain portions of the project)? If so, how are these limits documented and managed to ensure the individual's consent is reflected in practice. • Are consent documents written in plain language? • How long is consent valid? • What is the process for revoking consent? Privacy risks in this section include but are not limited to: • Consent practices: o High risk projects involve no consent, partial consent, lack of informed consent and/or consent is not documented.

	o Low risk projects exist when informed consent has been obtained and is in writing or verbal consent is well documented.

4. COLLECTION, USE, DISCLOSURE and/or RETENTION of PERSONAL and/or PERSONAL HEALTH INFORMATION

4	**Use and Disclosure** *USE* refers to handling, dealing with, applying or reproducing the information within a government institution. • Sections 5, 23 and 26 of HIPA sets out the legal authority for use of personal health information. • Section 28 of FOIP set out the legal authority for the use of personal information. *DISCLOSURE* is the sharing of information outside the government institution by any means e.g. faxing, mailing, electronically. • Section 5, 10, 23, 27 and 56 of HIPA set out the legal authority for disclosing personal health information. • Sections 29 and 30 of FOIP set out the legal authority for disclosing personal information. Please describe how the project will use and/or disclose information. Identify any privacy risks.
	Among other things, the description should answer the following questions: • Is the disclosure authorized by law? If so, please identify the provision(s) of the relevant legislation or regulations. • What are the planned uses of the information? o Do all the uses relate to the purpose of collection? o If secondary purposes are identified, is consent required? • Who will use the information? o What are the user's roles and permissions? Include a table if necessary. • Is the use authorized by law? If so, please identify the provision(s) of the relevant legislation. • Will the project disclose personal information or personal health information? o To whom, how and why is the information being disclosed?

	• Will any information be disclosed for common or integrated services?
	  o Are appropriate agreements in place?
	• Is shared information de-identified?
	• Is the minimum amount of information being used and/or disclosed?
	
	Privacy risks in this section include but are not limited to:
	• Access to identifiable information:
	  o High risk projects do not restrict access to project data and/or have unaudited access processes.
	  o Low risk projects grant access to project data on a demonstrated 'need to know' basis and regularly audit access.
	• Disclosure of identifiable information:
	  o High risk projects disclose identifiable information, do not rely on consent or have unclear authority for the disclosure.
	  o Low risk projects rely on consent or have clear authority for the disclosure of identifiable information or do not disclose identifiable information.

4. COLLECTION, USE, DISCLOSURE and/or RETENTION of PERSONAL and/or PERSONAL HEALTH INFORMATION	
5	**Retention** HIPA 17(2)(a) requires that personal health information stored in any format is retrievable, readable and useable for the purpose for which it was collected for the full retention period of the information. Clause 17(2)(b) requires that personal health information is destroyed in a manner that protects the privacy of the subject individual. Please describe how the project will retain and dispose of information. Identify any privacy risks.
	Among other things, the description should answer the questions: • Are a Records Retention and Disposal Schedule in place to manage records, including records containing personal information? [*The Archives and Public Records Management Act* s. 21, 22] • What types of records are generated by this system? • How are records stored and secured?

	• How will electronic records such as e-mails be retained and disposed of? Will they be stored in a way that they can be accessed, archived, and eventually destroyed even after employees leave government employment? What length of time will personal information and personal health information be retained for? Specify time period. Include any records management systems and schedules that are in place for retention of this type of information (for example, as found in your ARMS or ORS records management systems). • How are records to be securely disposed of? Privacy risks in this section include but are not limited to: • Records retention practices: o High risk projects do not have records retentions schedules and supporting policies and procedures in place. o Low risk projects have records retentions schedules in place that are supported by related policies and procedures. • Disposal of project information: o High risk projects do not have established procedures for the secure disposal of project data. o Low risk projects have established procedures for the secure disposal of project data.

5. ACCURACY AND CORRECTION	
1	**Accuracy and Correction** Section 27 of FOIP requires that government institutions ensure the personal information they use for *administrative purposes* is as accurate and complete as is reasonably possible. Section 31 of FOIP creates access rights for individuals whose personal information is contained in a record in the possession or under the control of a government institution. If an individual believes that a record containing their personal information contains errors or omissions, section 32 allows that individual to request that the record is corrected. Section 19 of HIPA requires a trustee must take reasonable steps to ensure that the personal health information the trustee collects is accurate and complete. Individual access rights under HIPA are established at section 32 and rights to request amendment to personal health information are established at section 40.

	Describe how individuals will be able to access and request correction or amendment of their information. Identify any privacy risks.

	When describing how individuals will be able to access and request correction or amendment of their information the description, among other things, should answer the questions:
	
	• What steps will be taken to ensure that any information collected is accurate, up-to-date and complete?
	• How will the project prevent accuracy errors?
	• How does the project confirm demographic information with the individual?
	• How are changes to information tracked?
	• What are the processes and procedures to provide access to the information?
	• Will individuals be able to request correction of their information?
	  o What procedures will be in place to accommodate these requests?
	
	Privacy risks in this section include but are not limited to:
	• Access and correction procedures:
	  o High risk projects do not have procedures in place to address requests to access information by individuals or address disputes regarding the accuracy of project information.
	  o Low risk projects have procedures in place which allow subject individuals to access the information about them that is being used in the project and dispute resolution mechanisms to address instances when the accuracy of information is in dispute.

6. SECURITY AND SAFEGUARDS

1	**Safeguarding** In the context of FOIP and HIPA, protection of privacy means the protection of personal information and personal health information. Trustees are required by section 16 of HIPA to protect the integrity, accuracy and confidentiality of personal health information. Physical, technical and administrative safeguards are ways in which government institutions protect personal information and personal health information. In the categories below describe the safeguards that the project will use to protect information. This description should identify how personal information will be protected against such risks as loss or unauthorized access, collection, use, disclosure, destruction, or modification.

	Identify privacy risks in each of the following areas. For each area privacy risks exist when safeguards that are reasonable for the sensitivity of the project information are lacking or are insufficient to protect project information. If more than one organization is involved the safeguarding practices of each organization should be considered.
2	**Physical Safeguards**
	• What physical safeguards are in place to protect the information? o Use of access cards; o Locked doors; o Security personnel; o Servers located in secure, climate controlled locations.
3	**Technical Security/Safeguards**
	• What technical safeguards prevent unauthorized user access to the system? • Is there a forced log out after a period of inactivity? • Are there password requirements set out in a policy or a standard? • Does the system capture user actions in audit trails? • What is tracked and logged?
4	**Administrative Safeguards**
	• Does your organization have privacy and security policies in place and available to all staff? • Do staff receive orientation and training on the policy? • Do staff sign an oath of confidentiality?

7. PRIVACY IMPACTS	
1	**Privacy Risks** Based on the information in the preceding section describe any identified privacy risks and what measures are currently in place to address them. If risks are not addressed a more in-depth PIA may be required. Describe any identified privacy risks and measures to address them.
	Among other things, the description should answer the questions: • Have any privacy risks been identified? If so please describe them. • What measures are in place to protect against the risks? • What measures are planned to address the risks?

8. CONCLUSION	
1	**Indicate whether or not a PIA is required/recommended and the reasons for the decision.**
	Yes
	No
	Unknown
Rationale	
Additional Information	

APPENDIX B
PIA REPORT TEMPLATE

PIA reports can be created in any format that best suits the needs of the government institution that the report is being prepared for. At a minimum, a PIA report should include the following areas:

Title Page

Include the project name, government institution/department, date and the identity of the person who completed the PIA process and prepared the PIA report.

Executive Summary

This section should:

- provide reviewers and decision-makers with an overview of the project;
- summarize your key findings, recommendations and action items; and
- note any outstanding privacy impact.

Table of Contents

Include main headings, sub-headings and appendices to enable reviewers to readily locate information.

Introduction

Explain:

- the objective of the project;
- the purpose of the PIA Report and the attached appendices; and
- the response being sought and timelines.

Background

Provide high-level context for your analysis and findings, including, but not limited to:

- PIA: Briefly describe the PIA process, including the purposes and outcomes of the preliminary analysis, project analysis and privacy analysis. Attach completed questionnaires, checklists and supporting documents;
- Scope: Briefly describe what is in-scope and out-of-scope in your PIA. Note any related projects, programs or systems, relevant PIA work or other risk analysis undertaken by other parties; and

- Glossary: Explain specialized terms and acronyms used in your PIA analysis and documentation.

Project

Provide a summary of the project including as much detail as is necessary to enable reviewers and decision-makers to understand the project in the context of your privacy analysis. Include the following, in addition to any specific information that you believe is necessary:

- description of the project;
- accountability for the project;
- related initiatives and linkages; and
- project partners and stakeholders.

Privacy

Provide context for your analysis of the project's impact on privacy, including, but not limited to:

- Personal Information: Briefly describe the type of personal information involved in the project and the individuals to whom it relates. Note whether the project will have a broad impact, involve significant amounts of personal information about any individuals or include sensitive information;
- Legislative Authority: Identify the legal authority for the project and for collecting, using and disclosing personal information. Include references to enabling legislation for the project, applicable privacy legislation (for example, FOIP or HIPA) and consents obtained.
- Safeguards: Identify any technical, administrative and physical safeguards in place to protect personal information and personal health information.
- Privacy Roles and Responsibilities: Identify the individuals and parties (internal and external to your institution) responsible for protecting privacy. Explain their roles and responsibilities; and
- Stakeholders: Identify relevant stakeholders and their importance to your privacy analysis. This can include involved areas within the government institution, partners in the delivery of programs and other individuals, groups or organizations which could be affected by the privacy risks. Indicate any consultation conducted or planned, the purpose and results.

Business Processes and Information Flows

You should explain relevant businesses processes, both existing and planned, including changes to existing processes, the key roles and responsibilities and the use of technology related to

those business processes. Identify who does what and why, when, where and how they do it.

Describe how personal information will flow through the business processes and technology; include the data elements that will be shared, with whom they will be shared, and the legal authority for sharing them. Describe how personal information will be collected, used, retained, disclosed, secured and disposed of, including changes to existing information flows, amounts or types of personal information involved and who will have access to the personal information and be responsible for it throughout its lifecycle.

Use plain language and organize this information in a way that makes sense for the project. For example, a complex project may need to provide an overview, as well as detailed descriptions of component parts.

Privacy Analysis

Explain the results of your completed privacy analysis, including:

- your findings;
- the privacy impact related to each finding;
- your recommendations on what needs to be done to protect privacy and comply with FOIP or HIPA; and
- priorities and proposed timelines and responsibility for implementation.

From this section, the reviewers and decision-makers should have a clear understanding of:

- the authority for the project (legislative and other instruments);
- the project's privacy risks;
- the work that needs to be undertaken to protect privacy and comply with applicable privacy legislation; and
- outstanding, remaining or unmitigated privacy risks and other issues impacting privacy.

Conclusions

Include any final remarks relevant to your PIA. For example, indicate whether the purpose of your analysis was successfully achieved or outstanding privacy work must be completed, etc.

Note key characteristics of the project including, but not limited to, whether it:

- could enhance privacy protection and ensure compliance with privacy requirements;
- could be designed to avoid, eliminate or reduce some/all of the identified privacy risks;
- could result in an unjustified invasion of privacy; or

- will involve new technology, business rules or processes for which the privacy risks are not known or well documented.

Next Steps

Highlight any required follow-up to your privacy analysis, such as the timing and priorities for implementing your mitigation strategy.

Approval

The project lead and other relevant decision-makers should approve the PIA Report acknowledging, in writing, that they understand the findings and recommendations and authorize implementation of the mitigation strategy/action items or acceptance of the privacy risks.

Attachments

Attach relevant documentation to support the findings and recommendations in this report. Examples of possible attachments include, but are not limited to:

- explanation of FOIP and HIPA provisions (e.g. possession or control and/or custody or control);
- list of documents reviewed and interviews conducted;
- copies of cited forms;
- summary of recommendations and action items; and
- completed PIA documents, including:
    - Preliminary Analysis;
    - Privacy Analysis Checklist; and
    - Project Analysis:
        - business process diagrams;
        - roles and responsibilities chart; and
        - information flow diagrams.

APPENDIX C
IMPACT FACTORS GUIDANCE TABLE

The table below is for demonstration purposes only. The factors faced by a government institution and the associated impact rank will vary amongst institutions based on their experiences, risk tolerance and other factors.

"Impact" Factors Guidance Table				
		Impact		
	Factors affecting the impact of a risk	High	Medium	Low
1.	Sensitivity of personal information	Identity information, financial information, biometrics, health information	Educational information, nationality; personal email addresses	personal opinions about low sensitivity topics (e.g. opinion on office space)
2.	Effect on individuals or third parties	Risk of identity theft, physical harm, hurt or humiliation, or risk to business opportunities	Pestered by marketers, inconvenienced	No effect or unnoticed
3.	Audience of unauthorized disclosures	101+ people	11-100 people	0-10 people
4.	Effect of Government's credibility or reputation	Legal ramifications, political ramifications, public outcry	Internal ramifications, major process overhauls	Expected, of little consequence

APPENDIX D
LIKELIHOOD FACTORS GUIDANCE TABLE

The table below is for demonstration purposes only. The factors faced by a government institution and the associated likelihood rank will vary amongst institutions based on their experiences, risk tolerance and other factors.

"Likelihood" Factors Guidance Table				
		Likelihood		
	Factors affecting the likelihood of risk materializing	High	Medium	Low
1.	Content is publicly available	No moderation or monitoring of content.	Content is monitored or moderated during business hours only.	All content is moderated and de-identified or redacted as needed before being publicly released.
2.	Group access to content	Open access.	Role-based access to all client files (i.e. all analysts can access any client file).	Need-to-know access to client files only (i.e. only assigned analyst can access client file).
3.	Technical security measures	No encryption, no password protection.	Password protection only.	All content in transit is encrypted and password protected.
4.	Physical security measures	Open, street access (no sign-in, no pass-cards). Open storage.	No identification needed for sign-in. Unescorted access.	Restricted, escorted access only.
5.	Policy	No access policies, no clear-set guidelines regarding information management. No existing policies.	Some policies in place, but no education on these policies.	Clear-set policies regarding information management and widespread education provided on these policies.