Logo

Description automatically generated

SantéSuite Inc.

Privacy Impact Assessment (PIA) Guide

Version 1.0

February 16, 2022

About This Guide

This Privacy Impact Assessment (PIA) Guide is intended to assist organizations with increasing awareness of privacy issues, especially in the context of the design and deployment of digital healthcare systems. This guide can also be used as background material when conducting a Privacy Impact Assessment for a project that will collect personal information. The companion *Privacy Impact Assessment Template* is also provided to provide a general framework for conducting a PIA.

Although the specific rules vary from jurisdiction to jurisdiction, we have tried to present a conceptual model that will apply to most environments.

Disclaimer of Warranties and Limitation of Liability

This information is provided as-is, and with no warranty as to the suitableness of the information to any given organization or situation. More specifically:

* The Licensor offers this Licensed Material as-is and as-available, and makes no representations or warranties of any kind concerning the Licensed Material, whether express, implied, statutory, or other. This includes, without limitation, warranties of title, merchantability, fitness for a particular purpose, non-infringement, absence of latent or other defects, accuracy, or the presence or absence of errors, whether or not known or discoverable.
* To the extent possible, in no event will the Licensor be liable to You on any legal theory (including, without limitation, negligence) or otherwise for any direct, special, indirect, incidental, consequential, punitive, exemplary, or other losses, costs, expenses, or damages arising out of use of the Licensed Material, even if the Licensor has been advised of the possibility of such losses, costs, expenses, or damages
* The disclaimer of warranties and limitation of liability provided above shall be interpreted in a manner that, to the extent possible, most closely approximates an absolute disclaimer and waiver of all liability

Table of Contents

[Introduction 4](#_Toc95923697)

[What is a Privacy Impact Assessment and what is its’ purpose? 4](#_Toc95923698)

[Legal Authority to Collect Personal Information 4](#_Toc95923699)

[Deciding to Conduct a PIA 5](#_Toc95923700)

[Information Sharing Agreements 5](#_Toc95923701)

[Conducting a Privacy Impact Assessment 6](#_Toc95923702)

[Step 1: Planning 6](#_Toc95923703)

[Step 2: Risk Analysis 7](#_Toc95923704)

[Limiting Collection 8](#_Toc95923705)

[Limiting Use 8](#_Toc95923706)

[Limiting Disclosure 9](#_Toc95923707)

[Data Retention & Disposal 9](#_Toc95923708)

[Accountability 9](#_Toc95923709)

[Transparency 10](#_Toc95923710)

[Data Accuracy 10](#_Toc95923711)

[Data Safeguards 10](#_Toc95923712)

[Step 3: Risk mitigation plan 10](#_Toc95923713)

[Step 4: Creating the Privacy Impact Assessment report 11](#_Toc95923714)

[Step 5: PIA Approval 11](#_Toc95923715)

[Step 6: PIA Publishing 11](#_Toc95923716)

[Step 7: Ongoing Review 11](#_Toc95923717)

[Appendix A: Risk Assessment Tools 13](#_Toc95923718)

[Risk Register 13](#_Toc95923719)

[Appendix B: Privacy Breach Examples 15](#_Toc95923720)

[References 16](#_Toc95923721)

# Introduction

In the digital age it has become easier than ever before to collect, store and analyze large sets of data about individuals – i.e. “personal information”. Personal Information (PI) is generally considered to be information about an individual that is recorded in any form and can include items such as name, address, employment history, biometric data, medical diagnoses, and even personal opinions. Although these data sets facilitate more efficient digital health systems and brings benefits to citizens, they also introduce potential privacy risks through misuse of that information. Many citizens feel that individual privacy is not a right that should be traded away in the name of innovation, efficiency, or commercial gain. In many jurisdictions protecting the privacy of personal information is also a legal requirement, in all jurisdictions it is essential to ensuring public trust in important institutions.

## What is a Privacy Impact Assessment and what is its’ purpose?

To understand and communicate the potential privacy impact that a new system may have, industry best practices call for a Privacy Impact Assessment (PIA) to be conducted. A PIA is a risk management process which assists in identifying and managing the privacy risks arising from the implementation of a new system. It helps institutions ensure that they meet any legislative requirements and identifies impacts that the new system may have on an individual’s privacy. This PIA process benefits the stakeholders of the new system in many ways, including reducing the risk of unauthorized collection, use, disclosure, retention or disposal of Personal Information. A PIA can never eliminate such risks altogether, however it can help to identify and manage those risks. In some jurisdictions PIAs have been mandated in certain situations.

What a PIA is not:

* a superficial legal checklist
* a one-time exercise
* a tool to hide risk and only show benefits of a project
* a justification for sub-standard policies or practices
* unnecessarily long, complicated, or difficult to read and understand

This guide provides a process and framework for conducting a Privacy Impact Assessment (PIA) for a jurisdiction that is considering or implementing a Master Patient Index or other related Digital Health System. We have also provided a companion PIA Template for jump-starting the PIA process.

## Legal Authority to Collect Personal Information

It is critical that any project determine the legal authority for the program or activity being conducted before considering whether you should undertake a PIA. If it is not clear that the project or program has the legal authority to collect Personal Information, you should not proceed with the initiative. The advice and direction provided in this document assumes that the legal authority to collect, use and disclose Personal Information has been granted to your project or program.

## Deciding to Conduct a PIA

In jurisdictions where conducting a PIA is not a legal requirement, other considerations may be used to decide whether or not to produce a PIA for a project or system deployment. Considerations may include:

* the sensitivity of the personal information being collected
* the number of people affected
* where there is government or public visibility into the project
* whether there is new or untested technology being used
* if the project is part of a broader strategic mandate
* there is a desire to follow industry best practices

In our experience conducting a PIA has many benefits for project stakeholders and we recommend to complete a PIA wherever practical. Even if you decide not to conduct a PIA, you should consider documenting your decision and rationale. You should always identify potential privacy impacts of your programs even if you do not conduct a formal PIA.

## Information Sharing Agreements

What does a PIA include?

The content that is included in a PIA will vary somewhat by local jurisdictional requirements and policy, however in general a PIA will include:

* a description of the activity or program and its’ objectives
* an assessment of your program’s potential impact on individual privacy
* an assessment of your program’s compliance to regulations and policy
* any measures planned to reduce privacy impact and to comply with regulations, policies, directions, guidelines and industry best practices

The length and content of your PIA will depend on the complexity and scale of your program.

# Conducting a Privacy Impact Assessment

This section describes the process for conducting a Privacy Impact Assessment (PIA). There are 7 steps to completing the PIA, they are: Planning, Risk Analysis, Risk Mitigation, Drafting, Approval, Reporting & Ongoing Review

## Step 1: Planning

The Planning phase involves collecting relevant information and scoping the project appropriately. First, it is recommended to determine the legal authority for the jurisdiction that the program or activity is being conducted. Next, it is recommended that the PIA activities are prioritized so that the activities that represent the greatest risk are assessed first. Ideally, the PIA is conducted early in the project lifecycle so that it is possible to offer suggestions to the program designers and that if negative privacy impacts are found that alternative approaches can be offered - it is always best to identify and mitigate privacy impacts before they occur. During the planning phase any published documentation about the program will be collected including business cases, previous assessments for the current program and/or related programs, analysis from the project teams, legal advice, institutional policies, etc. During this phase similar institutions in the region can also be contacted to gather examples of their PIAs.

During the Planning phase the scope of the PIA will be determined. The scope will identify what the PIA will cover, how detailed it needs to be and what areas are considered “out of scope”. It is important to identify and document what IS and what IS NOT being assessed and what aspects may impact privacy. The scope must include enough detail so that reviewers can assess risk to individuals - for example high level designs may not include information about which data fields are being conducted and will not reveal the true privacy impact of a program.

Planning will also include involving the right people. A list of stakeholders should be created, and a strategy for understanding when and how they should be involved should be created. Consider creating a RACI matrix for the PIA process which identifies who is Responsible, Accountable, Consulted, or Informed for each major deliverable. Especially important is to be clear about who is responsible for drafting the PIA and ultimately who will be responsible and accountable for ensuring that the privacy recommendations are implemented. Key parties to the PIA process include program staff that are responsible for designing and delivering the program or activity being undertaken, any internal privacy staff or groups or consultants, legal counsel, information management (IM) / information technology (IT) or information systems (IS) staff, end-users and front-line staff, third parties involved in the program, senior officials or executives accountable for the program. Not all of these parties are required to be engaged in every PIA and participation will vary by program.

Organizations may choose to conduct a multi-institutional PIA when two or more parties are co-delivering an initiative. These may be more economical and may also help to paint a more complete picture of the privacy impacts of a program. Multi-party PIAs help to reduce gaps in the analysis. A lead organization should always be appointed that holds the responsibility for completing the PIA.

Finally, the planning phase should establish a timeframe for the completion of the PIA.

## Step 2: Risk Analysis

Every activity conducted by an organization involves some sort of risk. Organizations manage risks by identifying them, analyzing them, and ultimately deciding whether or not a risk needs to be reduced or eliminated which is referred to as “mitigating”. Analyzing risks allows organizations to make choices about how programs are delivered when they involve various levels and types of risk. This analysis is intended to identify both the MOST SERIOUS and MOST LIKELY problems that a program will have. For each risk identified two metrics are derived:

1) the likelihood of an incident occurring and

2) the severity or impact on privacy rights and harm caused if it occurs

The likelihood of an event occurring ranges from rare (almost never likely to happen) to almost certain (happens all the time). The severity of the harm ranges from low (small impact) to large (devastating impact). The Risk Level for each identified risk is the mathematical product of the Severity and the Likelihood, i.e. :

**Risk Level = Severity \* Likelihood**

Note: it is worth mentioning that a PIA’s focus is on risk to privacy and that it is not a general risk assessment. Your program may require a more complete risk assessment which could include other types of risks such as patient harm due to clinical intervention, financial loss or other general losses.

When beginning the PIA, it is recommended that a *preliminary* risk assessment is completed. This will help to identify the general risk level of the program or project and indicate the depth and complexity that the privacy assessment will require. The higher the perceived risk, the more detailed of an analysis will be required and potentially more mitigations will be required. When completing the preliminary risk assessment the following risk factors should be considered:

* size of the population impacted
* amount of personal information being collected
* sensitivity of the personal information in the context of the program or region
* if the program will impact diverse groups in a biased fashion (certain genders or ethnicities for example)
* if the program will impact a vulnerable population
* type of potential impacts on individuals
* duration of activity or programs
* if the personal information is shared with other organizations or used for research, reporting or other secondary activities
* if the personal information is used to link the individual with other programs or services
* if the data is collected without consent of the individual
* if the data is used for policy-making
* if the data is used to make algorithmic or automated decisions
* if the data is used to monitor individuals

The length and complexity of the PIA process should reflect the risk level of the project being analyzed. A PIA for a low risk initiative could be a brief report, whereas a PIA for a program with a high privacy risk could be much more extensive. The impact to privacy rights of various groups should also be considered (gender groups for example) to understand how those groups may experience the program or initiative.

If, based on the information collected above, a preliminary assessment can be made that the initiative is simple and low risk, a simple PIA and brief report may be warranted. However if preliminary analysis indicates that the program is higher risk and/or privacy invasive then a more fulsome PIA with directed questions is warranted. Questions should be formed around the need for the program, and it’s impact in relation to it’s benefits. It is crucial to have these discussions early in the design of the program and not as an afterthought once the program is launched.

If a program is considered high risk, the following items should be considered:

* is the program necessary to meet a specific need? does it achieve a public goal or outcome?
* consider carefully the need for each specific element of personal information being collected and remove any that are not directly related to achieving the goal or outcome
* assess whether the benefits received by the program and in proportion to the potential privacy impact of the program
* consider whether or not the program is likely to be effective
* consider if there is an alternative way to achieve the same result with less privacy impact

**If an independent assessor cannot rationally explain how the proposed collection, use or disclosure of personal information is rationally connected to a proportional public goal, the initiative should likely NOT go ahead.** Any high-risk activity that proceeds should be able to effectively demonstrate that the program is necessary, minimally intrusive, likely to succeed and proportional to the privacy risk taken.

Please see Appendix A

### Limiting Collection

A core privacy principle is to only collect personal information that it is absolutely needed for a program to meet it’s objectives. A privacy risk review should scrutinize each piece of information by asking why it is needed – personal information should never be collected without a clear purpose. By avoiding collecting personal information unnecessarily, many inadvertent privacy risks can be avoided. Quite often information can even be collected without identifying individuals – this should be done where possible and this also helps to avoid privacy breaches.

### Limiting Use

Personal information should only be used for the purpose for which it was collected. The collection and use of this data must be clearly disclosed to the individual and their consent should be obtained where practical. Situations where personal information is used inappropriately for a secondary purpose or in a way that is contrary to the reasonable expectations of the individual should be avoided.

### Limiting Disclosure

Programs should avoid sharing of personal information collected about individuals. In situations where data is being shared, it should be clearly declared exactly which information is being shared, for what purpose and with whom it is being shared. Where practical, consent of the individual should be obtained Unauthorized use of personal information may occur when clear guidelines are not estavlished regarding the use of personal information. It is recommended that parties sharing information create data sharing agreement to document these terms.

### Data Retention & Disposal

Another core privacy principle is to only keep information for as long as it is needed. Clear guidelines for minimum and maximum retention periods and statements about individual programs should be established for the initiative that is collecting personal information around how long that data will be retained. A procedure for the notification of the end of a retention period and the secure destruction and verification of the deletion of the data should also be established, including electronic and paper copies and any backups or duplicates in existence (disaster recovery sites, etc.). Automation may be used here in certain cases to ensure timely deletion. Periodic spot-checks should be performed to ensure that data retention procedures are being followed. Personal information that is not disposed of properly may be accessed without authorization and may lead to a privacy breach.

### Accountability

Accountability means that a specific person or role is responsible for the handling of personal information, including developing policies, procedures and training of staff and contractors. Procedures should include instructions on how inquiries and complaints are received, investigated, assessed and responded to. Policies should publish information on who to contact regarding questions or concerns about privacy related matters. Policies should include information about training new staff or contractors. Organizations should document the official privacy complaint procedure and provide a form for complainants to use when filing an official complaint which captures the relevant information and timestamps the beginning of the process.

### Transparency

Whenever personal information is collected, it should be collected directly from the individual if possible. This ensures that the collection and exchange of data is minimized and that the data is up to date and accurate. Collecting directly from individuals also allows for an opportunity to explain the need for, and use of, the information. If appropriate, individuals can also be instructed on how to request updates or deletions of their data.

### Data Accuracy

Initiatives are responsible for ensuring that information stored about an individual is correct, especially when the individual’s personal information is being used to make a decision that directly affects them (ex. care decision). Programs should establish that there is a procedure for ensuring data quality and a process for correcting information where necessary. Groups should also periodically test the accuracy of information by doing spot-checks or audits. Ideally, participants should have an easy way to review, verify or correct the information stored about them.

### Data Safeguards

Any program that is collecting Personal Information must take steps to ensure that the information is appropriately protected from inappropriate access, use or disclosure. Safeguards should be established against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. Procedures should also be established for detecting and responding to these situations. Programs can use physical safeguards such as locked cabinets and rooms, as well as technical safeguards like audit trails and encryption to protect their information. Institutional safeguards such as training and documented procedures should also be used for maximum impact.

## Step 3: Risk mitigation plan

Once privacy risks have been identified during the analysis phase, the program must decide how to respond to those risks. Risk management varies by institution and program and will depend on the mandate and priorities of the organization as well as it’s level of risk tolerance and the interests of it’s partners, stakeholders, funders, etc. The risk mitigation response should produce an action plan which documents the decisions made about the various risks and the actions required to eliminate or minimize their impact. The action plan should clearly indicate the person or team responsible for its implementation, as well as a timeline for completion. Progress can be tracked against this plan as evidence of sound privacy management.

## Step 4: Creating the Privacy Impact Assessment report

The results of the previous phases should be documented in the privacy impact assessment report. The format of the report will vary depending on the size and complexity of the program being assessed. A report of this type should be concise and specific as well as readable by a wide variety of audiences. Health and technical acronyms and jargon should be avoided as the report may be accessed by an audience with a wide variety of backgrounds and even across jurisdictions. The PIA report should action-oriented towards the plan developed in Step 3. Wherever practical and appropriate PIA reports should be reviewed by external third parties to provide recommendations and to identify additional risks or gaps.

[treasury board secretariat directive on privacy impact assessment sets out content that must be included in PIA reports – find and use]

## Step 5: PIA Approval

What constitutes approval of a privacy impact assessment will vary dramatically depending on the circumstances of the program being assessed and the jurisdiction the program is to be launched. Appropriate internal and external stakeholder approvals including signatures should be sought, indicating that all parties are aware of and accept the risks and mitigations of the program.

## Step 6: PIA Publishing

Some jurisdictions consider publicly publishing their PIA reports (or sections or summaries of them) to be best practice as this allows individuals to have a basic understanding of how the programs are collecting and using their personal information. Reports should be edited to protect commercially protected information and/or program security as required.

## Step 7: Ongoing Review

Privacy risk analysis is an ongoing process that must continue throughout the lifetime of a program. Privacy issues should be re-assessed regularly, especially as the business, technical or regulatory environment changes. Some programs choose to schedule privacy checkpoints into their program or project plans to ensure that progress has been made with the privacy mitigations and to ensure that no significant changes have occurred during implementation (changes to UI, data feeds, integrations, etc.). PIAs can be modified and re-issued as appropriate, and they should always be considered living documents and contain the most up-to-date accurate information.

# Appendix A: Risk Assessment Tools

## Risk Register

One way to collect and analyze program risks is to create a *Risk Register* and to map the results into a *Risk Scoring Summary Matrix*. Please see below for examples of each.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk # | Description | Severity | Likelihood | Risk Score | Mitigation(s) |
| 1 | Accidental reveal of pregnancy status | Major | Possible | 12 | Only allow retrieval and display of this information inside local clinics |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Risk Scoring Summary Matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | **Severity** | | | | |
| 1  Negligible | 2  Minor | 3  Moderate | 4  Major | 5  Catastrophic |
| **Likelihood** | 5  Almost certain | 5 – Moderate | 10 – High | 15 - Severe | 20 - Severe | 25 – Severe |
| 4  Likely | 4 - Moderate | 10 – High | 12- High | 16 - Severe | 20 – Severe |
| 3  Possible | 3 - Low | 6 – Moderate | 9 – High | 12 – High | 15 - Severe |
| 2  Unlikely | 2 - Low | 4 - Moderate | 6 - Moderate | 8 – High | 10 – High |
| 1  Rare | 1 - Low | 2 - Low | 3 - Low | 4 - Moderate | 5 - Moderate |

# Appendix B: Privacy Breach Examples

This section provides some examples of situations that could result in the disclosure of, or access to, personal information by unauthorized parties:

1. The theft, loss or disappearance of equipment or devices containing personal information;
2. The sale or disposal of equipment or devices containing personal information without purging prior to sale or disposal;
3. The transfer of equipment or devices without adequate security measures;
4. The use of equipment or devices to transport or store personal information outside the office for telework or off-site work arrangements without adequate security measures;
5. The inappropriate use of electronic devices to transmit personal information, including telecommunication devices;
6. Intrusions that result in unauthorized access to personal information held in office buildings, file storage containers, computer applications, systems, or other equipment and devices;
7. Low level of privacy awareness among employees, contractors or other third parties that handle personal information;
8. Inadequate security and access controls for information in print or electronic format, on site or off-site;
9. The absence of provisions or inadequate provisions to protect privacy in contracts or in information-sharing agreements involving personal information;
10. Insufficient measures to control access and editing rights to personal information, which may result in wrongful access to, and the possible tampering with, records containing personal information;
11. “Phishing” - the use of deceptive tactics to trick an individual into providing their personal information either directly or by going to a fake web site. For example, an individual pretending to perform system maintenance calls an employee to obtain their security password; and
12. “Pharming” - the use of a fake copy of an official web site to redirect to a malicious web site in order to steal information without the user’s knowledge. For example, an individual accesses what he or she believes is an official web site and submits personal information as requested by the site. The individual is unaware that he or she has been redirected to a fake copy of the official web site.

# References

OECD. (2013). The OECD Privacy Framework. In *Organisation for Economic Co-Operation and Development*. https://www.oecd.org/sti/ieconomy/oecd\_privacy\_framework.pdf