Privacy Impact Assessment Guidelines

What is a privacy impact assessment (PIA)?

A PIA is an evaluation of a program to identify and help eliminate potential privacy risks and to ensure that PHI is being managed in accordance with the *HIA*. During this process, custodians take a close look at how they protect PHI as it is collected, used, disclosed, stored, and destroyed.

Acronym Alert:

HIA – Health Information Act

PHI – personal health information

PIA – privacy impact assessment

Why should we prepare a PIA?

It is far easier and less costly to address privacy issues proactively than to address it after a privacy breach has occurred.

When do we have to prepare a PIA?

The *HIA* requires that custodians prepare a PIA and submit it to the Commissioner for review and comment, in the following situations:

- For the new collection, use or disclosure of PHI or any significant change to the collection, use or disclosure of PHI;
- For the creation or significant modification to a PHI system or communication technology; or
- If a custodian performs data-matching.

A PIA **must** be completed and submitted to the Commissioner **before** the project is implemented.

What do we include in a PIA?

The *HIA* sets out information which is required to be in a PIA:

- How the proposed practices and systems relating to the collection, use and disclosure of PHI may affect the privacy of the individual to whom the PHI relates;
- If the custodian is data-matching then it must include:
    - How the PHI used in data-matching is to be collected;
    - How the PHI created through data-matching is to be used or disclosed.

How do we do a PIA?

There are ten basic principles that form the foundation of a PIA. These are sometimes called Fair Information Practices.

1. Accountability: Each custodian must put someone in charge of making sure privacy policies and practices are followed.
2. Identifying purposes: Individuals must be told why their PHI is being collected at, or before, the time of collection. You may consider, for example, posting notices.
3. Consent: Subject to some exceptions, individuals must give their consent to the custodian for the collection, use and disclosure of their PHI.
4. Limiting collection: Only PHI that is required may be collected.
5. Limiting use, disclosure and retention: PHI can only be used or disclosed for the purpose for which it was collected. Further consent is required for any other purposes. PHI should only be kept as long as necessary.
6. Accuracy: Custodians must use reasonable safeguards to ensure the accuracy of PHI.
7. Safeguards: Custodians must protect PHI from loss or theft. They must create safeguards to prevent unauthorized access, disclosure, copying, use or modification.
8. Openness: Custodians must make their privacy policies readily available to Individuals.
9. Individual access: Individuals have the right to ask to see their PHI held by a custodian. They have the right to know who the information has been given to, and can challenge the accuracy of PHI and ask for corrections.
10. Challenging compliance: Individuals must be able to challenge a custodian's privacy practices.

What do we send to the Commissioner?

The Commissioner will expect to see the following from a custodian:

- A cover letter signed by the custodian, which will address questions such as:
    - Does the custodian need the information?
    - Is the risk to privacy proportional to the need?
    - Is there a less privacy intrusive option?
- A detailed project overview including objectives, rationale, clients, programs and/or partners involved.
- A list of all stakeholders and their roles and responsibilities.
- A list of all data elements that involve PHI and a related description of the data flow.
- A list of relevant statutes and policies that govern the project to demonstrate legal authority for the collection, use or disclosure of PHI.
- A privacy analysis identifying privacy risks associated with the project. The Fair Information Practices should be addressed.
- A detailed plan to address privacy risks identified in the PIA.
- An outline of a breach response plan.
- Details on internal procedures relating to responding to access and correction requests, and complaints.

Format of a PIA

There is no single prescribed form for a PIA, as the complexity of a PIA will depend on the complexity of the activity. Applicants are welcome to search other jurisdictions for templates if they so choose.

What will the Commissioner do with our PIA?

The Commissioner does not approve projects or proposals, and we cannot draft PIAs for custodians. The Commissioner will review and comment upon your PIA, and may make recommendations under the *HIA*.