Managing a Privacy Program

EXERCISES with Answers

January 2015

***Please note that all of the scenarios and events portrayed in this document are fictitious.***

**SELF-ASSESSMENT QUIZ: How much do I know about managing a privacy program under the ATIPP?**
*Read the following questions and circle the correct answer. After 5 minutes, please be prepared to briefly introduce yourself and share your thoughts about the answer.*

|  |
| --- |
| Indicate whether the following statements are “True” or “False.”  |
| 1  | The functions in an Access and Privacy Program only need to reflect the structure and sections of the Act. | False |
| 2  | A public body isn’t required to have policy or process for access to information because requests are managed by the Records Manager.  | False |
| 3 | New hire privacy training is all that a public body needs to provide for its employees.  | False |
| 4 | Where a Privacy Officer is identified by position title, an individual acting in that position can exercise the powers of the position.  | True  |
| 5 | The ATIPP legislation serves as policy for a public body. | False |
| 6 | The Privacy Officer doesn’t need to be a lawyer or even an official of the legal department. | True |
| 7 | A public body is only required to protect the hard copy records it maintains on site in its offices.  | False |
| 8 | To avoid formal access requests, an organization can identify and disclose information ahead of time. | True |
| 9 | The initial implementation of policy and procedures completely satisfies a public body’s compliance. | False |
| 10 | If you have good security, you have good privacy. | False |

**EXERCISE 1**

A senior administrator working for a public body missed a meeting and found herself appointed Privacy Officer for the organization. Beyond an entry in the meeting minutes, there are no other documents or directives beyond the legislation to guide her in properly exercising this role. What are the highest priorities for this new Privacy Officer in establishing a proper access and privacy function?

**Answer:**

* Unless there is a clearly established mandate and job description for the role along with authorities for decisions and actions, the Privacy Officer will have difficulty fulfilling the duties of the job. This should be documented and authorized by the appropriate executive(s).
* Write and approve a set of policies documenting criteria, practices, and processes for access to information and protection of privacy. This will ensure that the organization has identified how the legislative requirements can be consistently and continuously implemented according to the unique functions and needs of the organization. Ensure that policy is backed up by appropriate sanctions.
* Establish goals and performance standards. Without these, the Privacy Officer will not be able to determine whether program policy, strategies, and operations are working. With this, the Privacy Officer can effectively report back to Senior Management to ensure buy-in and appropriate response to identified compliance risks.

|  |
| --- |
|  |

**EXERCISE 2**

You have been asked to set up some proactive disclosures or an Open Government initiative for your organization.

Questions:

1. What will be the objectives of such a program?
2. What information could be proactively disclosed and how will you determine that?
3. Will you meet resistance? If so, how will you handle it?
4. What existing services and systems can you leverage to establish and maintain the program?

**Answers**

1. What will be the objectives of such a program?
* Enhance accountability and transparency of government
* Encourage citizen engagement in government
* Better support for private and community organizations with government data about economics, usage, etc.
1. What information could be proactively disclosed and how will you determine that?
* Structured data: case information generated from a database
* Unstructured information: documents, files, e-mails, etc.
1. Will you meet resistance? If so, how will you handle it?
* Compliance with ATIPP (Section 64)
* Enhanced public trust
* Cost savings
* Better support for community
1. What existing services and systems can you leverage to establish and maintain the program?
* Records Management: records series descriptions and tracking
* Subject matter of formal access requests
* Website management
* IT systems development

**EXERCISE 3**

As the Privacy Officer you are visiting a branch office of your government organization to conduct some privacy awareness training for new employees. After finishing the training, you decide to do an informal walkabout to see how well the office is complying with Part 3 of the Act, especially section 33 (protection of personal information). As you wander around the office, you notice the following:

1. An employee is taking applications for a benefit program from individuals at the front counter in a busy reception area. You overhear the employee asking questions about the individuals’ income, assets, bank account, marital status, social service benefits, etc.
2. There is a small, empty conference room that is being used as an overflow coffee/lunch room.
3. Chairs for clients in the reception area are placed about 2 metres away from the front counter where interviews take place. There is also music playing from a sound system which tends to cover up conversations at the counter.
4. When one of the clients has finished the application interview, the front counter employee leaves the counter to look up the client’s previous file. She puts the client’s application in a folder and leaves the folder lying on the counter. The next client steps up to the counter waiting to be interviewed.
5. Completed client applications are sent to head office in a sealed envelope put inside an interoffice transit envelope.
6. There is a sign on a bulletin board that appears to be a notice about the collection of personal information. The board contains about 20 other notices.
7. The FAX and copier machines are shared with several other offices in the building. When you look into the room, there are several FAXES containing client information waiting to be picked up by staff of your public body and a FAX in the machine, sent by another office.
8. You know that there have been some incidents of theft in the office and that a surveillance camera has been installed above the front door of the office. The camera can only be seen if you are really looking for it. You do not see any notice informing the public that there is a camera on the premises being used for surveillance purposes.
9. A cardboard box marked “Confidential Shredding” sits under the front counter but you have not seen a shredder in the office.

After your tour, you ask the staff to join you for a quick meeting. What would you identify as actual or potential threats and risks to the privacy and security of client information? And what kind of safeguards or practices would you recommend be put in place to remedy the potential privacy breaches?

**Answer:**

1. Collecting sensitive personal information from clients in an open reception area leads to the risk of having other individuals eavesdropping. Your government organization is risking a privacy breach by allowing unauthorized access to personal information.
2. Priority for use of the small conference room should be given to interviewing /taking applications from clients.
3. By having space between the front counter and clients in the reception room, employees are attempting to protect client privacy and the confidentiality of their information. The question is whether 2 metres is sufficient to do this. Playing music in the reception area is another way that employees are trying to prevent eavesdropping. Consider painting a line 1-2 metres from the front counter and posting a sign that asks individuals waiting in the reception area to respect each other’s privacy by staying behind the line until they are called upon.
4. Placing the application in a closed folder signals to others that the information is probably private. However, this is only partially protecting privacy. By leaving a completed application on the counter in the open reception area, the employee has potentially disclosed personal information without any authority and risks having other clients or individuals access sensitive client information without authority. This information (such as bank account numbers or other financial information) could be stolen or misused for fraudulent purposes. There should be a policy in place so that no employee leaves this kind of personal information unattended, even in a closed folder. The applications should be removed from the counter or at least placed in closed folders under the counter, out of sight.
5. By putting the application form in a sealed envelope and then sending the sealed envelope in a separate transit interoffice envelope, the employees are ensuring that the privacy of clients is protected during transit from one office to another.
6. Although a collection notice has been posted on the bulletin board, unless a client was actually looking for it, he or she would likely not see it. Since employees are collecting personal information directly from individuals, the sign containing the notice should be clearly visible to clients before they start their interview; it should be drawn to their attention; or the collection notice should be printed and handed out to each client before employees start collecting information.
7. FAXES containing personal information should not be left in an area where they can be read by staff from other offices (unauthorized access). The office needs to establish some procedures for dealing with the shared FAX and copier situation or purchase a separate FAX machine. The office should have a schedule for checking the FAX machine regularly for incoming FAXES, particularly those containing personal information and for removing those promptly. If employees from other offices need to use the FAX and/or copier and are not part of a government organization under ATIPP, they may still be organizations that are subject to the *Personal Information Protection Electronic Documents Act (PIPEDA)* and will need to comply with the provisions in that Act for privacy and security of personal information in their custody or under their control. They would likely be willing to comply with some common procedures for protecting personal information whether it is in the custody or under the control of their organization, another organization or your government organization.
8. Collection of an individual’s image using a surveillance camera is considered a collection of personal information under the Act*.* Your government organization needs to have authority for the collection and there must be a notice setting out the authority and purposes for the collection and contact information of someone who can answer questions about the collection. Even if there was a good rationale and authority for installing the surveillance camera, the office still needs to establish policies for collection, use, disclosure, retention, security and disposal of the personal information collected by the surveillance camera.
9. Staff members should be able to tell you when and where the confidential material is shredded and what happens to the box when the office is closed. Just because the records have been assigned to the shredding bin does not remove the duty to protect them. The duty to protect continues until the records have been properly destroyed.

**EXERCISE 4**

If you were asked to conduct a comprehensive privacy compliance review of your organization, what questions would you ask, and based on what standards?

**Answer:**

**ATIPP Part 3 as a guide:**

* Has the department or agency identified a Privacy Officer?
* Is there authority for the collection of personal information and is all collection in line with this authority? (s. 29)
* Is the personal information collected directly from the individual(s) the information is about? (s. 30(1)) Is there a proper collection notice or notification of purpose? (s. 30(2))
* If not, is there authority under the Act for indirect collection? (s. 30(3))
* If decisions are made affecting individuals, are there reasonable efforts being made to ensure that the personal information used to make the decisions is accurate and complete? (s. 31)
* Are procedures in place to ensure that individuals can review their own personal and request correction or annotation in case of errors or omissions? (s. 32(1)) Are there procedures in place for correction or refusal of a correction to a record? (s. 32(2), (3), (4))
* Has your organization submitted general descriptions of the categories of records in the possession or under its control and the contact information for the appropriate officer for each institution included in the listing published by your government organization? (s. 63)
* Are policies and procedures in place to ensure that the personal information used in accordance with s. 35?
* Are the individuals responsible for disclosures of personal information trained and aware that disclosures fall within one of the provisions of section 36 or, if disclosure is for a consistent purpose, research purpose or archival purpose, does the disclosure comply with sections 37, 38 and 39 respectively?
* If personal information is used to make a decision about an individual, is it retained for at least one year from the date of the last use? (s. 34)

**Privacy Standards and Best Practices**

* Are reasonable security safeguards in place to protect the personal information against such risks as unauthorized access, collection, use, disclosure and destruction? Policy and procedures must cover the following areas:
	+ Administrative, physical and technical safeguards
	+ Threats and risks identified and mitigated
	+ Privacy policy established and communicated, including areas of Human Resources, IT, Records Management and Security, sanctions and penalties
	+ Privacy breach protocol established and well-known
	+ Complaints management protocol established and well-known
	+ Third party contractors sufficiently controlled
	+ Review and revision processes in place
* Conduct a site security review paying attention to:
	+ Physical security, identifying zones
	+ High risk records using information security classification
	+ Review of forms, collection instruments, collection notices
	+ User access management protocols
	+ Remote access protocols
* Determine whether a PIA should be completed on any existing or proposed additions or changes in systems or programs that affect the organization’s personal information collection, use, disclosure, storage or destruction?

**EXERCISE 5**

You are asked to develop privacy policies and procedures for your organization. In a group assigned by the facilitator, please draft an outline and/or a draft of one of the following:

* Privacy Officer Role Description

Policy:

* Scope
* Collection, Use and Disclosure
* Consent and Notice
* Accuracy
* Right of access and correction
* Retention and disposal
* Security
* Breach or complaints management