Completing a Privacy Impact Assessment

EXERCISES with Answers

January 2015

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

|  |
| --- |
| **QUIZ: Would I know when to do a PIA?** Indicate whether or not in the following circumstances if you would consider completing a PIA and briefly outline why.  |
| 1  | A public body is entering into a data matching project. | Yes |
|  | This will create new ways in which personal information is used and shared (disclosure). |  |
| 2  | A public body is moving its offices to a new location. | No |
|  | As long as the current systems and security measures remain the same, there would appear to be no changes in the way personal information is handled. |  |
| 3 | A public body is moving from paper and implementing an electronic record management system. | Yes |
|  | This may cause a change in the numbers or types of users, access to and security surrounding personal information. |  |
| 4 | The computer operating system is being upgraded, including software and bug fixes.  | No |
|  | This should not change the collection, use or disclosure of personal information.  |  |
| 5 | A public body has designated new information that may be released without an access request and is planning to post them on its web-site. | No |
|  | This should not involve the disclosure of any identifying personal information (otherwise there would likely be a contravention of the disclosure provisions of the ATIPP Act) so would not trigger the need for a PIA.  |  |
| 6 | All employees are going to be issued mobile phones and laptops with wireless network connections. | Yes |
|  | This will pose a multitude of issues including new risks to the access, use and security of personal information.  |  |
| 7 | A public body is hiring a new company to do general maintenance in all of its buildings. | No |
|  | The contract with the new company should be examined to ensure that the company is aware of its privacy and confidentiality obligations as a contractor to a public body and its employees should be signing confidentiality oaths. However this should not create any change to collection, use or disclosure of personal information. |  |
| 8 | A public body is creating a distance learning program.  | Yes |
|  | This will become a new collection of information from the public and may create issues with use, access and security. |  |
| 9 | The social committee is planning the summer BBQ and intends to post a list on which employees can make party suggestions.  | No |
|  | As long as posting is voluntary and employees are not asked for any highly sensitive personal information or given the opportunity to post anonymously, there are no privacy issues here.  |  |
| 10 | GPS systems are being added to all of the public body’s vehicles used by employees. | Yes |
|  | All surveillance and monitoring is a collection of personal information and this new collection would trigger the need for a PIA.  |  |
| 11 | You are creating a new position for an administrator who will have full access to client files and employee records.  | No |
|  | Hiring a new employee would not create any change to the handling of personal information. Ensure that all employees receive proper privacy training and sign any confidentiality oaths you have in place. |  |
| 12 | A public body is going to change its employee benefits provider. | No |
|  | As long as the benefits are being administered in a similar fashion ie. electronically, and the contract with the new provider ensures that the company is aware of its privacy and confidentiality obligations as a contractor to a public body and its employees should be signing confidentiality oaths, there should be no new privacy risks.  |  |
| 13 | A public body is hiring an outside contractor to run the government website. | No |
|  | Websites are not normally a place where personal information is collected, used or disclosed. However, specific provisions should be put in place for the protection of personal information if there is any collection through the web-site that has not been collected before by the public body. The contract with the provider should include clauses to ensure the provider is aware of its privacy and confidentiality obligations as a contractor to a public body and its employees should be signing confidentiality oaths, there should be no new privacy risks.  |  |
| 14 | A public body is planning to begin enumerating constituents online. | Yes |
|  | This is a collection of personal information in a new manner that could pose changes to the use, access and security of the personal information and would trigger the need for a PIA. |  |
| 15 | You are adding surveillance cameras to the outside and inside entrances of your office buildings. | Yes |
|  | All surveillance and monitoring is a collection of personal information and this new collection would trigger the need for a PIA. |  |

**EXERCISE 1**

You are asked to evaluate the risks involved in the following projects. What are the potential risks and how would you propose to reduce them?

1. Moving your public body’s records to a data warehouse (large database, typically housed on a cluster of servers, or a mini or mainframe computer, serving as a centralized repository of all data generated by all departments and units of an organization).

**Answer:**

Data warehouses may, over time, provide a venue for limitless data matching and creation of new forms of personal information inconsistent with client expectations. By their nature, data warehouses challenge or violate the basic privacy principles relating to limiting collection, disclosure, use, and obtaining consent for new uses. Thus, they entail a high degree of risk from a privacy perspective.

Risks must be carefully measured against the expected benefits to be derived from the data warehouse. In proceeding with the PIA, you should pay particular attention to any proposal to integrate personal data from separately legislated program databases or private sector databases.

The risks associated with data warehousing may be reduced in a number of ways, including:

* Consider products offering a single program database as an alternative to data warehousing;
* Anonymizing the data, thereby limiting potential threats to identification and privacy loss to a small number of individuals managing the data stripping or ID conversions;
* Providing value-added information services to interested parties instead of allowing direct access to identifiable data;
* Ensuring the custodianship and control of identifiable data remains subject to the ATIPP Act, and that such data are subject to frequent formal independent audits for compliance with project privacy and security standards.

Where such strategies are employed, the scope of the PIA will be significantly reduced.

1. Adding computer or kiosk-based transactions, automated voice response, call centres or remote access systems for members of the public to access your services.

**Answer:**

The shift toward new delivery channels can pose distinct challenges for security and privacy raising new issues with regard to client identification and authentication, and to the provision of notice or consent. Call centres, for example, may access program data for a range of programs, making data profiling both easier to perform and more difficult to detect. You may wish to preserve a range of access channels for service delivery, allowing customers to choose their preferred level of personal comfort, risk and convenience.

Wherever changes in delivery channels result in changes to how personal information is collected, used, or disclosed, a PIA will be required.

1. Developing a common (network) delivery system to allow for maximum access for use by many employees from any number of locations.

**Answer:**

Most common delivery systems maintain a central list of individuals authorized to access the system and their privileges. Most central listing activity is automated, and is designed to collect similar listings from linked or related systems that make it possible to find someone with an ID, electronic address, or privileges within the connected systems. This function is known as common directory services.

Where common directory services list personal information about individuals as customers of government programs, privacy issues may arise. This is particularly relevant in self-service electronic program delivery models, or where a directory is shared or aggregated between programs such that data profiling or data matching may be facilitated.

Wherever changes in delivery systems result in changes to who has access to personal information and how access is facilitated, a PIA will be required.

1. Outsourcing your IT services to a new company (alternate service delivery - ASD).

**Answer:**

Alternative service delivery (ASD) may raise a number of issues with regard to the protection of personal information. In assessing ASD arrangements, it is important to keep key differences between public and private sector service delivery in mind:

* Government has demand powers, which the private sector does not generally have;
* In most cases, there is the possibility of choice in consumer dealings with the private sector;
* The data being collected through these arrangements is, in many cases, more sensitive than data that would normally be collected by the private sector.

Depending on the sensitivity of the data, relatively straightforward out-sourcing of IT services or program intake functions where personal information is collected and processed on behalf of a public body and subject to FIPPA may not raise significant privacy issues.

In many cases, however, ASD arrangements are relatively complex and so require more careful scrutiny. Examples of such arrangements would include:

* Merging previously isolated transaction systems into a common governmental window,
* Localizing data collection activities through a common private sector window for previously isolated program data collections systems, which may also include concurrent data collection for private sector transactions,
* Materially changing the status of personally identifiable information, organizational accountability, and oversight of the business by accepted mechanisms such as internal/external auditors, the OIPC/Ombudsman.

Regardless of the specific details of the ASD arrangement, it is important that personal information continues to be protected when it passes into the hands of contractors and sub-contractors.

1. Adding service monitoring to measure public satisfaction and allocate resources by adding internet browser cookies and transaction logging.

**Answer:**

There is growing pressure for program areas to monitor service delivery in order to measure customer satisfaction and allocate resources. Careful system design can allow for monitoring with little or no privacy invasion. For example, Internet browser cookies and transaction logging systems can be designed and used to capture generic, non-identifiable or anonymized data which provides an adequate basis for service management without significant privacy risks. In such cases, a PIA will not generally be required.

Where service monitoring does involve the use of personally-identifiable data, however, a privacy impact assessment will likely be necessary.

|  |
| --- |
|  |

**EXERCISE 2**

Considering your public body’s personal information holdings generally, fill in the table below with the possible risks in each of the three categories, Administrative, Physical and Technical and then add the mitigation measures you would recommend.

**Privacy and Security Risks and Mitigation**

| ***Risks*** | ***Likelihood\**** | ***Harm\**** | ***Mitigation Measures*** | ***Rationale*** |
| --- | --- | --- | --- | --- |
| **Administrative*** Staff error
* Inconsistent practice
* Subjects not informed
* Staff don’t feel obligated to comply
* Ineffective incident response
* Ineffective request response
 |  |  | * Policies
* Staff Training/screening
* PIAs, PIRs
* Least amount, highest anonymity
* Records retrieval systems
* Subject notices/information
* Consents
* Sanctions, oaths
* Incident response procedures
* Event/disclosure logging
* Request procedures
 |  |
| **Physical*** Unauthorized external/internal physical access
* Loss in public area
* Unauthorized viewing
* Break-ins
* Equipment theft
* Incomplete destruction
* Mis-sent information
* Unauthorized destruction
* Wrong information destroyed
* Destruction by fires, disaster
* Environmental deterioration
 |  |  | * Secure storage
* Transport by secure containers
* Screens not in public view
* Locks/alarms
* Server/computers locked
* Data drive wiping/destruction
* Secure mail/courier
* Retention/destruction procedures
* Back-up procedures
* Recovery procedures
* Environmental controls
 |  |
| **Technical*** Unauthorized external/internal logical access
* Hacking or cracking
* Compromised authentication
* Hijacked transmissions
* Mis-sent transmission
* Virus attack
* Denial of service
 |  |  | * Firewalls
* Authentication
* Encryption
* Password controls
* Event logging
* Remote access controls
* Fax/e-mail security
* Virtual Privacy Network
* Virus protection
* UPS
 |  |
|  |  |  |
| ***\*Risk Levels*** | ***Likelihood***  | ***Harm***  |
| *Low* | Little possibility that the risk will occur due to mitigating factors | Compromise would likely not result in any significant harm to the privacy, safety, or economic standing of individuals or the corporation. |
| *Moderate* | A possibility that the risk will occur if no additional measures are taken. | Compromise would likely cause some harm to the privacy, safety, or economic standing of individuals or the corporation. |
| *High* | Near certainty that the risk will occur in the future if no corrective measures are taken. | Compromise would likely cause significant and immediate harm to the privacy, safety, or economic standing of individuals or the corporation. |

**EXERCISE 3**

Develop a Personal Information Flow Table for the following proposed program:

Many of your employees are required, as terms of their employment and according to various professional standards, to have certain training and certifications at the start and throughout their terms of employment in your public body.

You are implementing Continuing Professional Development standards for your employees to be managed electronically by Human Resources - Employment Services. The process will include the following:

* the collection of information about the employees’ current qualifications;
* the collection of the employees’ supporting documentation;
* undertaking and documenting an assessment of compliance;
* verification and periodic audits of compliance;
* confirmation and notification of compliance;
* notification of non-compliance and assisting employees in developing and submitting an action plan to become compliant; and
* initiation of a performance review/evaluation if the employee remains non-compliant.

Draft a Collection Notice to be used for the collection of personal information for this program.

**Answer:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *Flow #*  | *Description*  | *Type of Information* | *Purpose* | *Legal Authority* | *Custody or Control* |
|  *Continuing Professional Development (CPD)* |  |
| 1 | Employee discloses information about professional development | A. Demographics, B. Accreditations, certifications | Employee Services conducts Assessment for Compliance | Individual’s Own Personal informationATIPP Act s. 29(c) Collection | Individual EmployeeHuman Resources – Employee Services |
| 2 | Employee Services uses information provided by employee to assess compliance | A. Employee name, contact information, B. Accreditations, certifications | Completion of Compliance Assessment | ATIPP Act S. 35(1)(a) Use | Human Resources – Employee Services |
| 3 | Employee discloses to and Employee Services collects supporting documentation from employee for verification and audit purposes | A. Employee name, contact informationB. Accreditations, certifications and information contained in supporting documentation | Completion of Verification and Audit to determine compliance | Individual’s Own Personal InformationATIPP Act s. 29(c) Collection | Human Resources – Employee Services |
| 4 | Employee Services uses information gathered during Verification and Audit to assess Member compliance. | A. Employee name, contact information B. Accreditations, and certificationsC. Employee Services Audit | Continuing employment if compliant | ATIPP Act S. 35(1)(a) Use | Human Resources – Employee Services |
| 5 | Employee Services uses information from Verification and Audit to assess Member compliance | A. Employee name, contact information B. Accreditations, and certificationsC. Employee Services Audit | Non-compliance may trigger Performance Review. | ATIPP Act S. 35(1)(a) Use | Human Resources – Employee Services |
| 6 | Employee discloses requirements to Employee Services and Employee Services collects Action Plan from Employee | A. Employee name, contact information B. Action Plan | Development and implementation of Action Plan to allow employee to achieve and maintain compliance | Individual’s Own Personal InformationATIPP Act s. 29(c) Collection | Individual EmployeeHuman Resources – Employee Services |

**Collection Notice:**

Your name, business contact information and accreditation and certification information are collected under the authority of the Access to Information and Protection of Privacy Act (Yukon) S. 29(c). This information will be used in the administration of the Human Resources Continuing Professional Development Program. If you have any questions about the collection of your personal information for this program, contact the World’s Most Awesome Privacy Officer, 123 Maple Street, Whitehorse, YK, wmapo@gov.yk.ca or 867.123.4567.