Privacy Compliance Tool

Checklist

Prepared by:

Ombudsman Manitoba

October 2003

PRIVACY COMPLIANCE TOOL

CHECKLIST

INTRODUCTION:

This "Checklist" should be used in conjunction with the Privacy Compliance "Guide". The "Guide" provides general information and explanations that are helpful in completing the "Checklist",[1] contains many relevant legislative references, and provides some "best practices" that may be useful for building privacy awareness into organizations and projects.

The purpose of the "Checklist" is to provide a diagnostic process for privacy compliance that covers the basic requirements of sound information privacy practices. It is designed to assist organizations evaluate the privacy compliance of a program, a specific initiative, a policy or an information system. Each of the main sections or Elements of the "Checklist" reflects a major privacy process or issue (e.g. limiting *use*, *disclosure*, and retention). By answering the specific questions related to each privacy element, managers and supervisors will be able to review practices and determine what action may be needed to initiate or improve compliance.

Users are asked to offer an **Explanation** for each answer and to provide **Attachments** or an action plan if applicable. **Action Plans** provide detail on corrective or developmental actions that need to be taken (e.g. develop a training program to provide privacy and security awareness for staff).

The "Checklist" also contains the basic requirements for compliance and may be used by the Ombudsman's Office as a basis for privacy audits or investigations.

Please note that throughout the text of the "Checklist" and "Guide", certain words or terms may be italicized to indicate that they are defined in *Appendix 1* to the "Guide". Italics are also used for some subheadings and for references to statutes. We have also provided the "Checklist" in summary form ("Checklist at a Glance") as an overview of the process and a tally of responses to the questions.

Some words of advice:
take the time to read over the "Guide" before using the "Checklist".

[1] The following Privacy Impact Assessments and Diagnostic Tools assisted in the preparation of this Privacy Compliance Tool: Office of the Privacy Commissioner for Personal Data, Hong Kong, "Privacy Safe" 2000 (available http://www.pco.org.hk/); Ontario Management Board Secretariat: Electronic Service Delivery Privacy Standard (2000) and Privacy Impact Assessment Guidelines (1999) (available at www.gov.on.ca/mbs); Privacy Commissioner of Ontario: Privacy Diagnostic Tool (2001) (available at: www.ipc.on.ca); Privacy Commissioner of Alberta: Privacy Impact Assessment Template (2001) (available at http://www.oipc.ab.ca/).

TABLE OF CONTENTS

CHECKLIST FOR THE PRIVACY COMPLIANCE TOOL:

PROJECT INFORMATION

Date:
Name of Organization and Program Area:

CONTACT INFORMATION

Name:
Telephone and FAX:
Address:
E-mail:

(**NOTE:** the "contact" should be the person most qualified to respond to questions regarding the compliance assessment.)

DESCRIPTION OF PROGRAM/SYSTEM OR OTHER INITIATIVE

Describe the mandate and functions of the organization and program area or initiative being assessed for privacy compliance (be sure to identify specific legislative authorities if applicable):

Provide details of any privacy impact assessments or other forms of *personal information* or *personal health information* assessments already conducted on this program or initiative:

ELEMENT 1

IDENTIFYING PURPOSES AND LIMITING COLLECTION OF PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

This Element of the "Checklist" is designed to determine if the collection of *personal* and *personal health information* you undertake is authorized by FIPPA or PHIA and if the information you collect is limited to the purposes identified by the organization. The Element requires that you:

Identify the Purpose for which the information is collected at or before the time it is collected (FIPPA s.36(1)), or before it is collected or as soon as practicable afterward. (PHIA s.15(1))

Limit Collection of the information to that which is necessary for the purposes identified by the organization. (FIPPA s.36(2), PHIA s.13(1) and (2))

Collect information directly from the individual unless indirect collection is authorized according to the legislation. (FIPPA s.37(1), PHIA s.14(1) and (2))

Inform (notify) the individual, when collecting directly, of the purpose, legal authority (when FIPPA is involved), and provide contact information of an official who can answer queries about collection. (FIPPA s.37(2), PHIA 15(1))

Privacy Compliance "Checklist"

1. There is a detailed description of the type of *personal information*, *personal health information* or personal data elements collected for this program or initiative.

Yes ☐ **No** ☐	
Explanation:	
Attachment ( ) or Action Plan ( ):[2]	

[2] Please mark with an "X" in parentheses if included with this assessment.

2. The purpose for collecting this *personal information* is authorized according to FIPPA. It is:
   a. authorized by an enactment of Manitoba or Canada, or
   b. directly related to and is necessary for a program or activity of the *public body*, or
   c. necessary for law enforcement or crime prevention.

   NOTE: please specify whether (a), (b), or (c) above applies, and if it is (a), identify the enactment(s) and applicable section(s).

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

3. *Personal health information* is not collected unless it is:
   a. for a lawful purpose connected with a function or activities of the trustee; and,
   b. is necessary for that purpose.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

4. *Personal* or *personal health information* is collected only directly from the subject individual or his or her authorized representative.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

5. If *personal information* or *personal health information* is collected indirectly (i.e. from a third party), the *indirect collection* is authorized under Section 37(1) of FIPPA or Section 14 of PHIA.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

6. Individuals are informed (notified) of the purpose, authority (where FIPPA is involved) for *collection*, and how to contact an officer or employee who can answer their questions about the *collection*.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

ELEMENT 2

LIMITING USE, DISCLOSURE, AND RETENTION OF PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

This Element is designed to determine if *personal* and *personal health information* is used or disclosed only for the purposes for which it was collected (or as otherwise authorized under Part 3 of FIPPA or of PHIA), and is retained only in accordance with a written retention and disposal policy that conforms with legal requirements.

If information is used or disclosed for another purpose, then either the *consent* of the individual is required or a law must require or permit that *use* or *disclosure*.

This Element also encompasses certain uses and disclosures of *personal information*, not otherwise authorized under FIPPA, that may or must be submitted to the Privacy Assessment Review Committee (PARC) process under Sections 46 and 47. It further deals with the disclosure of *personal health information* for health research under PHIA Section 24. The Introduction to the "Guide" provides additional important detail not repeated here and should be consulted to understand the questions more fully.

Note that *personal* and *personal health information* "sharing" and "exchange" are not concepts defined in FIPPA and PHIA. If the *disclosure* of such information forms part of an *Information Sharing Agreement*, the agreement must comply with the provisions of the Acts.

Users of the "Checklist" should note that Part 3 of FIPPA does NOT apply to *personal health information*. Also, when considering "Checklist" item A1 immediately following, FIPPA s.43(c) should be consulted for further guidance about the limits on permitted *use* of *personal information* and PHIA s.21 for details about restrictions on the *use* of *personal health information*.

Privacy Compliance "Checklist":

A. Limiting *Use*

1. *Personal information* or *personal health information* is used only for the purpose for which it was obtained, or for a *use* consistent with that purpose under FIPPA, or directly related to that purpose under PHIA.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):[3]	

[3] Please mark with an "X" in parentheses if included with this assessment.

2. *Consent* is obtained from the individual before using *personal information* for a purpose NOT consistent with the original purpose for which it was collected or, in the case of *personal health information*, for a purpose NOT directly related to the original purpose for which it was collected.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

3. There is a list of the staff positions or categories that use this *collection* of *personal* or *personal health information*.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

4. Physical, administrative, and technical controls limit access to identifiable *personal* and *personal health information* to those who have a "need to know".

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

5. The least amount of *personal* and *personal health information* is used to meet the stated purpose.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

6. *Personal* or *personal health information* is used with the highest degree of *anonymity* to meet the stated purpose.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

B. Limiting *Disclosure*:

1. Individual *consent* is obtained before disclosing *personal* or *personal health information* to another government department or agency, *local public body*, *trustee* or other third party.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

2. If *consent* is not obtained, the *disclosure* is authorized according to a specific provision of Section 44(1) of FIPPA or Section 22(2) of PHIA.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

3. When *disclosure* is required and authorized, the amount and type of information disclosed is limited on a "need to know" basis.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

4. *Disclosure* is made at the highest degree of *anonymity* possible while still meeting the purpose of the recipient.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

5. Staff maintains a *disclosure* log or audit trail of:
   a. what information has been disclosed,
   b. to whom it has been disclosed, and
   c. the purpose and authority for the *disclosure*.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

C. *Uses* and *Disclosures* of *Personal Information* Not Otherwise Authorized under Division 3 of FIPPA

1. **For a *public body*** other than a *local public body* under Section 46 of FIPPA:

   The proposal or request has been referred to the Privacy Assessment Review Committee[4] (PARC) for its advice
   a. if the proposed *use* or *disclosure* is not otherwise authorized under Division 3, and involves *data linking* or *data matching* of *personal information* in one database with another, or
   b. if the request is for disclosure on a bulk or volume basis of *personal information* in one public registry or another collection of *personal information*.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

[4] The Privacy Assessment Review Committee (PARC) is established under FIPPA s.77. The committee reviews requests for uses or disclosures of *personal information* that involve *data matching* or *data linking*, bulk disclosures and research requests. PARC provides advice to the Head of the public body under sections 46 and 47 of FIPPA.

2. **For a *local public body*** under Section 46 of FIPPA:

   The proposal or request has been either assessed internally by the *local public body* or referred to the Privacy Assessment Review Committee (PARC) for its advice
   a. if the proposed use or disclosure is not otherwise authorized under Division 3, and involves *data linking* or *data matching* of *personal information* in one database with another, or
   b. if the request is for disclosure on a bulk or volume basis of *personal information* in one public registry or another collection of *personal information.*

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

3. For *uses* or *disclosures* by *public bodies* contemplated under Section 46 of FIPPA, the Head of the *public body* or *local public body* has considered advice received through the statutory privacy assessment review process and approved conditions that must be met under Section 46(6), <u>including a written agreement</u> with the recipient of the *personal information.*

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

D. Disclosure of *Personal Information* for a Research Purpose under FIPPA

1. The Head of the *public* or *local public body* has considered any privacy assessment advice requested under Section 47(2) of FIPPA and approved conditions that must be met under Section 47(4), including a written agreement with the recipient of the *personal information.*

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

E. Disclosure of *Personal Health Information* for a Research Purpose under PHIA

1. The *personal health information* required for the health research project is recorded information about an identifiable individual that relates to
   a. the individual's health, health history (including genetic information about the individual), or
   b. the provision of health care to the individual, or
   c. the payment of health care provided to the individual, and includes
   d. the Personal Health Identification Number (PHIN) and any other identifying number, symbol or particular assigned to an individual, and
   e. any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

2. The health research project has been approved according to the requirements of PHIA Section 24 by
   a. the Health Information Privacy Committee[5] (HIPC) if the *personal health information* is maintained by the government or a government agency, and
   b. an institutional research review committee if the *personal health information* is maintained by a *trustee* other than the government or a government agency.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

3. The researcher and the *trustee* have entered into an agreement under PHIA Section 24(4), and any regulations, in which the researcher agrees
   a. not to publish the *personal health information* in an identifying form,
   b. to use the *personal health information* only for the purposes of the approved research project,
   c. to ensure that reasonable safeguards are in place to protect the security and confidentiality of the *personal health information*, and
   d. to ensure that the information will be destroyed or deidentified at the earliest opportunity consistent with the purposes of the project.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

[5] The Health Information Privacy Committee is established under Section 59 by the Minister of Health to approve research projects under Section 24 of PHIA and to perform any other functions assigned to it by the Minister.

F. Limiting Retention:

1. There is a written records/data retention policy that meets all relevant legislative requirements.

Yes ☐ **No** ☐	
Explanation:	
Attachment ( ) or Action Plan ( ):	

2. *Personal* or *personal health information* used to make a decision that directly affects an individual is retained for a reasonable period of time to allow the individual to obtain access to it.

Yes ☐ **No** ☐	
Explanation:	
Attachment ( ) or Action Plan ( ):	

ELEMENT 3

ENSURING ACCURACY OF PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

These questions are designed to determine whether *personal* or *personal health information* collected is as accurate, complete, up-to-date, and not misleading as is necessary for the purposes for which it is to be used. (FIPPA s.38, PHIA s.16)

1. There are procedures in place to verify *personal* or *personal health information* and to manage requests for corrections that comply with FIPPA Sections 38 and 39 or with PHIA Sections 16 and 12.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):[6]	

2. The authority to modify or correct *personal* or *personal health information* is clearly established to ensure that those without this authority may not or are unable to alter these records.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

[6] Please mark with an "X" in parentheses if included with this assessment.

3. An audit trail is maintained to document when and by whom a file or record was compiled or updated.

Yes ☐ **No** ☐	
Explanation:	
Attachment ( ) or Action Plan ( ):	

ELEMENT 4

SAFEGUARDING PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

Organizations are required to protect *personal* and *personal health information* by making reasonable security arrangements against risks such as unauthorized access, *use*, *disclosure*, or destruction. These security requirements apply to records in hard-copy form as well as to records that are kept electronically, such as a database. While the general security requirements for hard copy and electronic records are the same, the implementation of safeguards will differ. Therefore, the questions have been organized to address the general and then the specific, implementation requirements. (FIPPA, s.41; PHIA Part 3, Division 2 and Regulation 245/97)

The basic security requirements or safeguards for *personal health information* are laid out in more specific detail in PHIA Sections 18, 19, and the Regulations than for *personal information* under FIPPA (Section 41). Nevertheless, the intent is the same under both statutes: to ensure reasonable security arrangements are in place for personal data regardless of the physical form or characteristics of the information medium. Both Acts have specific regulation-making power for security matters, but only PHIA has specific regulations at this time (Spring 2003).

A Privacy Compliance "Checklist"

1. Security measures are in place for *personal* and *personal health information* regardless of media format (i.e. paper, photographic, electronic, etc.).

Yes ☐	**No** ☐
Explanation	
Attachment ( ) or Action Plan ():[7]	

2. Written information security policies include a definition of roles and responsibilities, and sanctions for breaches of policy.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

[7] Please mark with an "X" in parentheses if included with this assessment.

3. Staff receives ongoing training about security policies and procedures, and is made aware of the importance of security and *confidentiality* on an ongoing basis.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

4. Security breaches and violations are documented, responded to, and corrective measures taken according to established processes.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

5. Access to *personal* or *personal health information* is regularly monitored and audited.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

6. *Personal* and *personal health information* are stored or maintained in a physically secure location.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

7. *Personal* and *personal health information* in all media are disposed of securely to prevent unauthorized access.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

8. Physical removal of *personal* and *personal health information* of any medium from a secure designated area is always undertaken in a manner and in accordance with procedures that continue to ensure the security of the information at all times.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

B Electronic Systems Security:

1. Users are assigned unique user identifications and passwords for access to personal data, and passwords are changed regularly.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

2. Network and application security status is assigned on a "need to know" basis according to the particular requirements of specific roles within the organization.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

3. Access privileges are revoked promptly when required (e.g. when an employee leaves or moves).

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

4. Systems contain audit trails for tracking data access and audit logs provide information about abnormal or unusual access.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

5. Access logs and audit trails are reviewed on a regular basis.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

6. *Personal* and *personal health information* is transmitted by secure means to minimize opportunities for unauthorized or accidental interception by third parties.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

7. Virus protection is implemented and an effective firewall is in place where necessary, for all information systems that contain *personal* or *personal health information*.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

8. External providers of information management or technology services are covered by written agreements dealing with risks including unauthorized access, *use*, *disclosure*, retention, and destruction or alteration as required under FIPPA Section 44(2) and PHIA Section 25(3).

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

ELEMENT 5

ENSURING INDIVIDUAL ACCESS TO PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

An individual, or his/her *authorized representative*, is entitled to have access to information about the *personal* and *personal health information* an organization holds about him/her. (FIPPA Part 2, PHIA Part 2) An organization should be prepared to explain how *personal* and *personal health information* are used and disclosed. (FIPPA Part 3, ; PHIA Part 3)

Privacy Compliance "Checklist"

1. A process to respond to access requests under the Act(s) is in place.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):[8]	

2. Individuals are informed that the organization holds *personal* or *personal health information* about them and that access to that data is provided, except in limited circumstances as defined in legislation.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

[8] Please mark with an "X" in parentheses if included with this assessment.

3. Requests for access are responded to within the legal time limits at minimal or no cost, or in compliance with legislation.[9]

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

4. The requested information is provided in an understandable format and the organization is prepared to explain any terms or abbreviations.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

5. A refusal to grant access to all or part of an individual's information includes the specific provision for refusal under the legislation and clear reasons for the refusal.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

[9] FIPPA Regulation 64/98 sets the chargeable fees under this Act. PHIA s.10 states that a trustee may charge a reasonable fee for permitting examination of *personal health information* and providing a copy, but the fee must not exceed the amount provided for in the regulations. PHIA did not have a fee regulation as of Autumn 2003.

ELEMENT 6

CHALLENGING COMPLIANCE

People have the right to question public bodies and trustees about their compliance with the information privacy protection provisions under FIPPA and PHIA. It is extremely important that the public's right to make complaints about alleged infractions of the legislation is made known on a timely basis to individuals. The right to challenge compliance is one of the fundamental tenets of internationally accepted principles of fair information practices.

Privacy Compliance "Checklist"

1 There are communication policies and procedures in place that ensure individuals are routinely informed that they may make a complaint to the organization and are informed about their statutory right to make a complaint to the Manitoba Ombudsman respecting their *personal* and *personal health information* rights.

Yes ☐ **No** ☐	
Explanation:	
Attachment ( ) or Action Plan ( ):[10]	

[10] Please mark with an "X" in parentheses if included with this assessment.

ELEMENT 7

ACCOUNTABILITY AND OPENNESS OF POLICIES AND PRACTICES

An organization is responsible for *personal* or *personal health information* in its custody or under its control, and specific individuals are designated by law, regulation or policy to be accountable for the organization's compliance with established privacy principles. (FIPPA Sections 80, 81, Regulation 64/98 Sections 1, 2; PHIA Sections 57, 58)

Under FIPPA Section 75, a *public body* must make certain basic information relating to the management of *personal information* available to the public.

Privacy Compliance "Checklist"

1. It is understood and known in the organization that the Head of a provincial government department or agency, or the Head of a *local public body*, or a *trustee* is accountable for compliance with access and privacy legislation, and that any delegation of powers and duties should be formally recorded.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):[11]	

2. An employee (or employees) within the organization is formally delegated responsibility for the daily administration of privacy compliance ("access and privacy coordinator" under FIPPA, "privacy officer" under PHIA). The identity of the individual(s) is known throughout the organization.

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

[11] Please mark with an "X" in parentheses if included with this assessment.

3. There are written organizational policies and procedures that define the responsibility for protecting *personal* and *personal health information.*

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

4. Appropriate staff is provided with on-going training to implement privacy policies and procedures.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

5. Other parties, such as *information managers* and agents, who may have authorized access to *personal* or *personal health information* under Parts 3 of FIPPA or PHIA are aware of, and comply with, organizational privacy policies and relevant procedures.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

6. Individuals can obtain information about privacy policies and procedures with reasonable ease.

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

7. Under FIPPA, *Personal Information Banks* have been identified, described, are up-to-date, and publicly available as required. [Note that PHIA does not have a corresponding provision in relation to production of a directory including a description of personal information banks.]

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

8. Under FIPPA and in the case of a *public body* that is not a *local public body*, (1) a record is kept of uses and disclosures not included in the publicly available "Access and Privacy Directory", (2) this record is attached or linked to the *personal information* involved, and (3) a process is in place to have this information included in the "Access and Privacy Directory". [Note that PHIA does not have a directly corresponding provision.]

Yes ☐ **No** ☐
Explanation:
Attachment ( ) or Action Plan ( ):

9. A procedure exists for responding to questions or concerns about privacy practices.

Yes ☐ **No** ☐	
Explanation:	
Attachment ( ) or Action Plan ( ):	

ELEMENT 8

ASSESSING PRIVACY RISKS IN ELECTRONIC SERVICE DELIVERY (ESD)

Ideally, privacy implications should be considered at the earliest stages of electronic service delivery (ESD) systems design. To avoid potentially costly modifications, fair information practices must be considered in the concept and system definition phases, and continue during the decision-making about use of the data through to final systems design and approval. A privacy impact assessment by the client organization is often an indispensable front-end part of the process, but it is important to recognize that the assessment needs to evolve with the system and be an integral reference point for subsequent maintenance and upgrades.

Privacy assessments should also be considered for existing systems, particularly when they are subject to major maintenance work or are being upgraded.

The principles reflected in Elements 1-7 of this Privacy Compliance Checklist may form the privacy-planning framework for policy choices and ESD technical design. PHIA and FIPPA do not in themselves restrict organizations to specific technologies or modes of delivery, but the organizations are expected to follow and be able to demonstrate informed decision-making where ESD systems will process *personal* and *personal health information*.

The questions in Element 8 will help determine whether privacy risks associated with electronic service delivery have been considered. They are intended to support the analysis of both simple and complex electronic service delivery options. These options include delivery of services through the public service administration, through private sector channels, or through public-private partnerships.

NOTE: *Explanations and/or Action Plans should be provided for all questions contained in this Element, regardless of a "yes" or "no" response.*

Privacy Compliance "Checklist"

1. Are diagrams available to illustrate the flow of *personal* and *personal health information* for this project?

Yes ☐ **No** ☐	
Explanation:	
Attachment ( ) or Action Plan ( ):[12]	

[12] Please mark with an "X" in parentheses if included with this assessment.

2. Has responsibility for control and custody for all *personal* or *personal health information* processed by the ESD system been identified and assigned?

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

3. If the ESD system will process transactions for more than one program, agency or department, have constraints been placed on data integration?

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

4. If this ESD project involves the use of common identifiers or a common identification infrastructure, have privacy-enhancing measures been considered to limit risks to privacy?

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

5. Will this ESD initiative require *data linking* (data profiling) *or data matching*?

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

6. Is there a means of obtaining, authenticating, registering and maintaining individual *consent* electronically, where required?

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

7. Have privacy-enhancing technologies and/or techniques been considered for this ESD project?

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

8. Have all the risks to privacy for this ESD initiative been identified and documented?

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

9. Have all risks to privacy for this ESD project been minimized or averted?

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

10. Has a comprehensive risk analysis been undertaken to identify and implement appropriate ongoing monitoring and regular auditing requirements to protect *personal* and *personal health information*, including that of end-users, for all aspects of the ESD system?

Yes ☐	**No** ☐
Explanation:	
Attachment ( ) or Action Plan ( ):	

11. Have key stakeholders been consulted about the privacy implications of this project?

Yes ☐ **No** ☐	
Explanation:	
Attachment ( ) or Action Plan ( ):	

12. Where risks to privacy are not completely mitigated, is there a strategy for responding to public concerns over privacy protection?

Yes ☐ **No** ☐	
Explanation:	
Attachment ( ) or Action Plan ( ):	

13. Have constraints been placed on ESD service providers regarding the *collection*, *use* and *disclosure* of information subject to FIPPA or PHIA?

Yes ☐ **No** ☐	
Explanation:	
Attachment ( ) or Action Plan ( ):	

14. Do all contracts related to the implementation of this ESD project contain data protection provisions?

Yes ☐ **No** ☐	
Explanation:	
Attachment ( ) or Action Plan ( ):	