

PHIA Privacy Compliance Tool

Checklist at a Glance

PHIA PRIVACY COMPLIANCE TOOL

CHECKLIST AT A GLANCE

INTRODUCTION

The purpose of this summary form of the larger PHIA Privacy Compliance "Checklist" document is to provide users with a quick overview of the questions included in the privacy assessment. This document will facilitate keeping a record of answers and assessing overall compliance. The "Checklist at a Glance" includes all the questions, but no explanatory notes. It will help the user keep track of explanations, attachments, and action plans that are included with the full "Checklist".

Users should provide an explanation for each "no" answer and an attachment or action plan if applicable. *Attachments* offer additional information on what exists (e.g. a security policy) whereas *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).

NOTE: The italicized terms are defined in the "Guide" at "Appendix 1", "Common Terms and Definitions".

TABLE OF CONTENTS

CHECKLIST AT A GLANCE FOR THE PHIA PRIVACY COMPLIANCE TOOL

ELEMENT 1: Identifying Purposes and Limiting Collection of Personal Health Information	6
ELEMENT 2: Limiting Use, Disclosure and Retention of Personal Health Information	7
ELEMENT 3: Ensuring Accuracy of Personal Health Information	9
ELEMENT 4: Safeguarding Personal Health Information.....	10
ELEMENT 5: Ensuring Individual Access to Personal Health Information	12
ELEMENT 6: Challenging Compliance	12
ELEMENT 7: Accountability and Openness of Policies and Practices.....	13
ELEMENT 8: Assessing Privacy Risk in Electronic Service Delivery	14

ELEMENT 1

IDENTIFYING PURPOSES AND LIMITING COLLECTION OF PERSONAL HEALTH INFORMATION

LEGEND:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;

"A/AP?" = Attachment or Action Plan?

			Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. There is a detailed description of the type of <i>personal health information</i> , or personal data elements collected for this program or initiative.						
2. <i>Personal health information</i> is not collected unless it is: <ul style="list-style-type: none"> a. for a lawful purpose connected with a function or activities of the <i>trustee</i>; and, b. is necessary for that purpose. 						
3. <i>Personal health information</i> is collected only directly from the subject individual or his or her authorized representative.						
4. If <i>personal health information</i> is collected indirectly (i.e. from a third party), the <i>indirect collection</i> is authorized under Section 14 of PHIA.						
5. Individuals are informed (notified) of the purpose for <i>collection</i> , and how to contact an officer or employee who can answer their questions about <i>collection</i> .						

ELEMENT 2

LIMITING USE, DISCLOSURE AND RETENTION OF PERSONAL HEALTH INFORMATION

LEGEND:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;

"A/AP?" = Attachment or Action Plan?

Expl? A/AP?

A. Limiting Use

1. *Personal health information* is used only for the purpose for which it was obtained or for a *use* directly related to that purpose under PHIA.
2. *Consent* is obtained from the individual before using *personal health information* for a purpose NOT directly related to the purpose for which it was collected.
3. There is a list of the staff position or categories that use this collection of *personal health information*.
4. Physical, administrative, and technical controls limit access to identifiable *personal health information* to those who have a "need to know".
5. The least amount of *personal health information* is used to meet the stated purpose.
6. *Personal health information* is used with the highest degree of *anonymity* to meet the stated purpose.

B. Limiting Disclosure

1. Individual consent is obtained before disclosing *personal health information* to another government department or agency, *local public body, trustee* or other third party.
2. If *consent* is not obtained, the *disclosure* is authorized according to a specific provision of Section 22(2) of PHIA.
3. When *disclosure* is required and authorized, the amount and type of information disclosed is limited on a "need to know" basis.
4. *Disclosure* is made at the highest degree of *anonymity* possible while still meeting the purpose of the recipient.
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*.

Y	N	Y	N	Y	N

LEGEND:

" Y " = Yes; " N " = No; " Expl? " = Explanation?;
 " A/AP? " = Attachment or Action Plan?

Expl? A/AP?

C. 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.

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

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.

D. Limiting Retention:

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

2. *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.

	Y	N	Y	N	Y	N

ELEMENT 3

ENSURING ACCURACY OF PERSONAL HEALTH INFORMATION

LEGEND:

" Y " = Yes; " N " = No; " Expl? " = Explanation?;
 " A/AP? " = Attachment or Action Plan?

Expl? A/AP?

	Y	N	Y	N	Y	N
1. There are procedures in place to verify <i>personal health information</i> and to manage requests for corrections that comply with PHIA Sections 16 and 12.						
2. The authority to modify or correct <i>personal health information</i> is clearly established to ensure that those without this authority may not or are unable to alter these records.						
3. An audit trail is maintained to document when and by whom a file or record was compiled or updated.						

ELEMENT 4

SAFEGUARDING PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

LEGEND:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
 "A/AP?" = Attachment or Action Plan?

	Expl?		A/AP?	
	Y	N	Y	N
1. Security measures are in place for <i>personal health information</i> regardless of media format (i.e. paper, photographic, electronic, etc.).				
2. Written information security policies include a definition of roles and responsibilities, and sanctions for breaches of policy.				
3. Staff receives ongoing training about security policies and procedures, and is made aware of the importance of security and <i>confidentiality</i> on an ongoing basis.				
4. Each employee and agent has signed a pledge of confidentiality that includes an acknowledgement that he or she is bound by the trustee's written security policy and procedures and is aware of the consequences of breaching them.				
5. Security breaches and violations are documented and responded to according to established processes.				
6. Access to <i>personal health information</i> is regularly monitored and audited.				
7. <i>Personal health information</i> is stored or maintained in a physically secure location.				
8. <i>Personal health information</i> in all media is disposed of securely to prevent unauthorized access.				
9. Physical removal of <i>personal health information</i> 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.				

Electronic Systems Security:

LEGEND:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
 "A/AP?" = Attachment or Action Plan?

Expl? A/AP?

	Y	N	Y	N	Y	N
1. Users are assigned unique user identifications and passwords for access to <i>personal health information</i> , and passwords are changed regularly.						
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.						
3. Access privileges are revoked promptly when required (e.g. when an employee leaves or moves).						
4. Systems contain audit trails for tracking data access, and audit logs provide information about abnormal or unusual access.						
5. Access logs and audit trails are reviewed on a regular basis.						
6. <i>Personal health information</i> is transmitted by secure means to minimize opportunities for unauthorized or accidental interception by third parties.						
7. Virus protection is implemented and an effective firewall is in place where necessary, for all information systems that contain <i>personal health information</i> .						
8. External providers of information management or technology services are covered by written agreements dealing with risks including unauthorized access, <i>use, disclosure</i> , retention, and destruction or alteration as required under PHIA Section 25(3).						

ELEMENT 5

ENSURING INDIVIDUAL ACCESS TO PERSONAL HEALTH INFORMATION

LEGEND:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
 "A/AP?" = Attachment or Action Plan?

	Expl?		A/AP?	
	Y	N	Y	N
1. A process to respond to access requests under the Act is in place.				
2. Individuals are informed that the organization holds <i>personal health information</i> about them and that access to that data is provided, except in limited circumstances as defined in legislation.				
3. Requests for access are responded to within the legal time limits at minimal or no cost, or in compliance with legislation.				
4. The requested information is provided in an understandable format and the organization is prepared to explain any terms or abbreviations.				
5. A refusal to grant access to all or part of an individual's information includes clear reasons for the refusal.				

ELEMENT 6

CHALLENGING COMPLIANCE

LEGEND:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
 "A/AP?" = Attachment or Action Plan?

	Expl?		A/AP?	
	Y	N	Y	N
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 <i>personal health information</i> rights.				

ELEMENT 7

ACCOUNTABILITY AND OPENNESS OF POLICIES AND PRACTICES

LEGEND:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
 "A/AP?" = Attachment or Action Plan?

Expl? A/AP?

	Y	N	Y	N	Y	N
1. It is understood and known in the organization that the <i>trustee</i> is accountable for compliance with access and privacy legislation, and that any delegation of powers and duties should be formally recorded.						
2. An employee (or employees) within the organization is formally delegated responsibility for the daily administration of privacy compliance ("privacy officer" under PHIA). The identity of the individual(s) is known throughout the organization.						
3. There are written organizational policies and procedures that define the responsibility for protecting <i>personal health information</i> .						
4. Appropriate staff is provided with on-going training to implement privacy policies and procedures.						
5. Other parties, such as information managers and agents, who may have authorized access to <i>personal health information</i> under Part 3 of PHIA are aware of, and comply with, organizational privacy policies and relevant procedures.						
6. Individuals can obtain information about privacy policies and procedures with reasonable ease.						
7. A procedure exists for responding to questions or concerns about privacy practices.						

ELEMENT 8¹

ASSESSING PRIVACY RISKS IN ELECTRONIC SERVICE DELIVERY (ESD)

LEGEND:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
 "A/AP?" = Attachment or Action Plan?

Expl? A/AP?

	Y	N	Y	N	Y	N
1. Are diagrams available to illustrate the flow of <i>personal health information</i> for this project?						
2. Has responsibility for control and custody for all <i>personal health information</i> processed by the ESD system been identified and assigned?						
3. If the ESD system will process transactions for more than one program, agency or department, have constraints been placed on data integration?						
4. If this ESD project involves the <i>use</i> of common identifiers or a common identification infrastructure, have privacy-enhancing measures been considered to limit risk to privacy?						
5. Will this ESD initiative require <i>data linking</i> (data profiling) or <i>data matching</i> ?						
6. Is there a means of obtaining, authenticating, registering and maintaining individual <i>consent</i> electronically, where required?						
7. Have privacy-enhancing technologies and/or techniques been considered for this ESD project?						
8. Have all risks to privacy for this ESD initiative been identified and documented?						
9. Have all risks to privacy for this ESD project been minimized or averted?						
10. Has a comprehensive risk analysis been undertaken to identify and implement appropriate ongoing monitoring and regular auditing requirements to protect <i>personal health information</i> , including that of end-users, for all aspects of the ESD system?						
11. Have key stakeholders been consulted about the privacy implications of this project?						
12. Where risks to privacy are not completely mitigated, is there a strategy for responding to public concerns over privacy protection?						
13. Have constraints been placed on ESD service providers regarding the <i>collection, use</i> and <i>disclosure</i> of information subject to PHIA?						
14. Do all contracts related to the implementation of this ESD project contain data protection provisions?						

¹ Users are asked to provide **Explanations and/or Action Plans** for ALL questions contained in this Element, regardless of a "yes" or "no" response. **Attachments** offer additional information on what exists (e.g. a security policy) whereas **Action Plans** provide details on corrective or developmental actions that need to be taken (e.g. develop a training program and provide privacy and security training for staff).