Manitoba
Health, Seniors and Active Living

POLICIES & PROCEDURES
UNDER
THE PERSONAL HEALTH INFORMATION ACT

"The PHIA Manual"

Approval Date: November 5, 2014
Revision Date: May 2, 2018

Table of Contents

INTRODUCTION

Manitoba Health, Seniors and Active Living (the Department) collects, maintains, uses and discloses personal health information daily. In many cases, these functions are necessary for program and service delivery, yet they must take place within an environment that respects and protects the rights of access to information and protection of privacy.

The Personal Health Information Act (PHIA) was proclaimed December 7, 1997. As of that date, the Department has a statutory responsibility to grant access to personal health information, upon request, and to protect the privacy of the personal health information in its custody and control. The PHIA Manual has been developed to ensure that the Department's information practices are in keeping with these statutory obligations, as well as any amendments to the Act that will occur from time to time.

The PHIA Manual includes the global policies and procedures for the Department under *The Personal Health Information Act* (PHIA). As per Section 6 of the Personal Health Information Regulation, the Department is required to ensure that all departmental employees and agents receive orientation and ongoing training regarding these policies and procedures (see Policy X: PHIA Orientation and Ongoing Training).

The PHIA Manual recognizes that branches may need to further develop or refine their own policy and procedural requirements to address their unique circumstances. Branches should develop their own written policies and procedures and train branch employees and agents in them so that they are aware of the specific policies and procedures to be followed regarding the specific personal health information within that branch. Branches are also encouraged to review any other existing branch policies that are already in place to ensure they are PHIA compliant.

For more information on this Manual, PHIA orientation and ongoing training, or *The Personal Health Information Act* in general and how it effects the operation of the Department and its respective branches/units, contact:

Legislative Unit
204-788-6612

DEFINITIONS

Agent: (Section 1 of the Personal Health Information Regulation)
In relation to a trustee, includes:

(a) if the trustee is a corporation, an officer or director of the corporation, and
(b) a student or volunteer.

Demographic Information: (Section 1(1) of PHIA):
Means an individual's name, address, telephone number and e-mail address.

Personal Health Information (PHI): (Section 1(1) of PHIA)
Means recorded information about an identifiable individual that relates to:

(a) the individual's health, or health care history, including genetic information about the individual
(b) the provision of health care to the individual, or
(c) payment for health care provided to the individual

and includes

(d) the 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

Representative: (Section 60 of PHIA)
The rights of an individual under PHIA may be exercised

(a) by any person with written authorization from the individual to act on the individual's behalf
(b) by a proxy appointed by the individual under *The Health Care Directives Act*
(c) by a committee appointed for the individual under *The Mental Health Act* if the committee has the power to make health care decisions on the individual's behalf
(d) by a substitute decision maker for personal care appointed for the individual under *The Vulnerable Persons Living with a Mental Disability Act* if the exercise of the right relates to the powers and duties of the substitute decision maker
(e) by the parent or guardian of an individual who is a minor, if the minor does not have the capacity to make health care decisions, or
(f) if the individual is deceased, by his or her personal representative (defined in *The Trustee Act* as the Executor or Administrator of the individual's estate)

If the trustee believes that no person listed above exists or is available, the adult person listed first in the following clauses who is readily available and willing to act may exercise the rights of an individual who lacks the capacity to do so:

(a) the individual's spouse, or common-law partner, with whom the individual is cohabiting
(b) a son or daughter
(c) a parent, if the individual is an adult
(d) a brother or sister
(e) a person with whom the individual is known to have a close personal relationship

(f) a grandparent
(g) a grandchild
(h) an aunt or uncle
(i) a nephew or niece

The older or oldest of two or more relatives described above is to be preferred to another of those relatives.

Trustee: (Section 1(1) of PHIA):
Means a

a) health professional
b) health care facility
c) public body, or
d) health services agency

...that collects or maintains personal health information.

As the Department is a public body that collects and maintains personal health information, it is a trustee under PHIA.

POLICY I: Access to Personal Health Information

Policy

It is the policy of the Department, as a trustee under *The Personal Health Information Act* (PHIA), to assist individuals in exercising their right of access to personal health information (PHI) maintained by the Department. The Department will:

1) give notice to individuals of their right to examine and receive a copy of their personal health information maintained by the Department, and about how they can exercise that right
2) inform individuals of their right to authorize another individual to exercise their PHIA rights, and
3) assist individuals in exercising their right of access to personal health information maintained by the Department

Procedure

Definition of Access

For the purposes of PHIA and this policy, "access" refers to an individual's right to examine or receive a copy of his/her recorded personal health information. The right of access applies only to the individual the information is about or his/her representative. Providing personal health information to any other third party is considered a disclosure and is covered in POLICY IV: Disclosure of Personal Health Information.

Notice of Right to Access

In accordance with the Personal Health Information Regulation, the Department must take reasonable steps to inform individuals of their right to examine and receive a copy of their personal health information that the Department maintains, and about how they can exercise that right.

To this end, the Department will:

- post information on its website setting out:
    - what types of personal health information the Department maintains
    - that individuals have the right to examine and receive a copy of their PHI, and
    - how to exercise those rights
- display the poster "Your Information, Your Privacy" in publicly accessible areas of the Department, and
- generally assist individuals in exercising their right of access to personal health information

Requests for Access

A Personal Health Information Access Request Form must be submitted to the Department in writing by the individual the information is about, or his/her representative.

The request must include the following information:

- the full name, address, phone number and personal health identification number (PHIN) of the person whose information is being requested
- the extent or nature of the information being requested
- the date of the request
- if the person submitting the request is not the individual the information is about, any supporting documentation setting out their authority to access the information, and
- the signature of the individual whose information is being requested (or his/her representative)

Any employee who receives a request for access to information under PHIA will, as soon as practicable, forward the request to the appropriate branch in the Department for consideration and processing.

Transferring a Request

Upon receiving a request for access, the Department must identify whether the request should be transferred to another trustee. This must be determined and executed within 7 days of receiving the request.

Before transferring a request, the Department will consider its general duty to assist and any potential frustration to the individual that may result from a transferred request.

A request for access to information under PHIA may be transferred if:

- the personal health information is maintained by another trustee, or
- another trustee was the first to collect the personal health information

When a request for access is transferred, the Department must simultaneously notify the individual that the transfer has been made.

If an access request is transferred to the Department by another trustee, the Department must respond as promptly as possible as but no later than 30 days after receiving it.

Responding to Requests for Access

The Department must respond to a request for access as soon as possible, but in any case, must respond within 30 calendar days of receiving the request (unless a transfer is made in accordance with the previous section). A failure to respond within this timeframe may be considered a refusal of access. The individual can then proceed to the Ombudsman with a complaint.

The Department must respond to a request for access in one of the following ways:

- by making personal health information available for examination or by providing a copy, if requested, to the individual
- by informing the individual in writing if the information does not exist or cannot be found, or
- by informing the individual in writing that the request is refused, in whole or in part, citing the specific reason(s) for refusing access, and advising the individual of his/her right to make a complaint to the Ombudsman about the refusal

Each branch must maintain a tracking log of requests for access under PHIA and responses.

Reasons for Refusing Access

The Department can refuse access to portions of an individual's personal health information if one of the following circumstances exists:

- knowledge of the information could reasonably be expected to endanger the mental or physical health or the safety of the individual or another person
- disclosure of the information would reveal personal health information about another person who has not consented to the disclosure
- disclosure of the information could reasonably be expected to identify a third party, other than another trustee, who supplied the information in confidence under circumstances in which confidentiality was reasonably expected
- the information was compiled and is used solely:
    - for the purpose of peer review by health professionals
    - for the purpose of review by a standards committee established to study or evaluate health care practice in a health care facility or health services agency
    - for the purpose of a body with statutory responsibility for the discipline of health professionals or for the quality or standards of professional services provided by health professionals
    - for the purpose of risk management assessment, or
- the information was compiled principally in anticipation of, or for use in, a civil, criminal or quasi-judicial proceeding

Severance

If the Department determines that access to a portion of the personal health information should be refused, that information must be "severed" (ex: blacked out) from the information that the individual is permitted to access, and then the individual must be permitted to examine or be provided a copy of the remainder of the information.

Precautions on Release of Information

The Department must not permit personal health information to be examined or copied without first being satisfied as to the identity of the individual making the request.

The Department must also take reasonable precautions to ensure that the personal health information is received by the intended recipient. Refer to POLICY VIII: Security of Personal Health Information for information regarding the secure transmission of PHI.

Making Information Available for Examination

If the individual asks to view or examine the information, the Department will arrange a time for the viewing and will have an employee present to provide the individual with any assistance requested.

If the information is maintained in electronic form, a printed copy of the information will be made available for viewing. Individuals will not be permitted to view his or her information using an employee's computer.

Duty to Provide an Explanation

The Department must be prepared to provide the individual with an explanation of any terms, codes or abbreviations used in his/her personal health information.

Fees

Upon receiving a request for access, the Department will notify the individual of any costs associated with examination and obtaining copies of personal health information.

Branches are permitted to charge the fees prescribed under the Access and Privacy Regulation of *The Freedom of Information and Protection of Privacy Act* (Appendix A: Access Fee Schedule) for facilitating examination and providing copies of personal health information.

Accessibility

When providing access under this policy, branches must consider any requirements of *The Accessibility for Manitobans Act,* the Customer Service Standard Regulation under that act and the departmental policy titled Access to Manitoba Health Publications, Events and Services for Persons with Disabilities.

Responsibility

Branches are ultimately responsible for processing and responding to requests for access under PHIA.

Branch leads are responsible for ensuring that this policy is followed.

Each branch must maintain a tracking log of requests for access under PHIA and responses.

The Legislative Unit will provide assistance to branches where required.

Authority

The Personal Health Information Act – Sections 5, 6, 7, 8, 9, 9.1, 10 and 11

Effective Date:

October 1, 2003

Revision Date:

May 2, 2018

POLICY II: Correction of Personal Health Information

Policy

It is the policy of the Department, as a trustee under *The Personal Health Information Act* (PHIA), to assist individuals in exercising their right to request corrections to their personal health information maintained by the Department.

Procedure

Requests for Correction

Individuals have a right to request a correction to their recorded personal health information. All requests for correction must be submitted to the Department using the Personal Health Information Correction Request Form.

Any employee who receives a request for correction to personal health information will, as soon as practicable, forward it to the branch that maintains the information for consideration and processing.

Responding to Requests for Correction

The Department must respond to a request for correction as soon as possible, but in any case, within 30 calendar days of receiving the request.

The Department must respond to a request for correction in one of the following ways:

- by making the correction and notifying the individual that it has been made
- by informing the individual that the correction cannot be made because the information no longer exists or cannot be located
- by informing the individual the Department does not maintain the information and by providing him/her with the name and address (if known) of the person/trustee who does maintain the information, or
- by informing the individual that the request for correction has been denied and following the steps outlined in the Refusing a Request for Correction section below

Considering a Request for Correction

When determining whether to make a correction, the Department must consider the nature of the information in question. Where the Department is notified that information it maintains is factually incorrect (such as an inaccurate birth date, gender, or PHIN) the Department will make every effort to comply with the request. Where the Department is asked to make a correction to information compiled based on professional judgement (such as a clinical diagnosis or an opinion about an individual's suitability or eligibility for a program) the Department may or may not determine that the suggested correction is appropriate.

Making a Correction

When making a correction, the Department must:

- add the new information to the original record so that it will form part of the record, or
- where adding the information is not possible, ensure that the original record is clearly cross-referenced with the corrected information

If the information to be corrected was disclosed to another trustee or person during the preceding year, the Department must, when practicable, notify that trustee or person that a correction has been made.

Refusing a Request for Correction

When the Department determines that a correction will not be made, the Department must:

- permit the individual to file a concise statement of disagreement describing the requested correction and the reason for the request
- add the statement of disagreement to the record in such a way that it will be read and form part of the record or be adequately cross-referenced to it
- when practicable, provide a copy of the statement of disagreement to any other trustee or person to whom the personal health information has been disclosed during the preceding year, and
- inform the individual of his/her right to make a complaint to the Manitoba Ombudsman

Receiving a Notice of Correction or Statement of Disagreement

Any employee who receives notice about a correction or statement of disagreement shall, as soon as practicable, forward it to the branch that maintains the information for consideration and processing.

Fees

The Department is not permitted to charge a fee for receiving, processing or responding to a request for correction to personal health information, whether or not the correction is made.

Responsibility

Branches are ultimately responsible for processing and responding to requests for corrections, and for adding a statement of disagreement where required by this policy.

Branch leads are responsible for ensuring that this policy is followed.

The Legislative Unit will provide assistance to branches where required.

Authority

The Personal Health Information Act – Section 12

Effective Date:

October 1, 2003

Revision Date:

June 1, 2017

POLICY III: Collection of Personal Health Information

Policy

It is the policy of the Department, as a trustee under *The Personal Health Information Act* (PHIA), to limit its collection of personal health information in accordance with the requirements of PHIA.

Procedure

Collection

The Department will only collect personal health information if:

- the collection is for a lawful purpose connected with a legitimate activity or function of the Department, and
- the collection of the information is necessary for that purpose

Restrictions on Collection

The Department will limit its collection of personal health information to the minimum amount of information it requires. Each branch must determine the minimum amount of personal health information necessary for its authorized program activities and functions.

Source of Information

The Department will collect personal health information directly from the individual the information is about unless one of the following exceptions exists:

- the individual has authorized another method of collection
- collection of the information directly from the individual could reasonably be expected to endanger the mental or physical health or the safety of the individual the information is about
- collection of the information is in the interest of the individual and time or circumstances do not permit collection directly from the individual
- collection of the information directly from the individual could reasonably be expected to result in inaccurate information being collected
- the information is collected for the purpose of
    i. compiling an accurate family or genetic health history of the individual, or
    ii. determining or verifying the individual's eligibility to participate in a program of or receive a benefit or service from the trustee or from the government, and is collected in the course of processing an application made by or on behalf of the individual, or
- another method of collection is authorized or required by a court order or an enactment of Manitoba or Canada

When a branch collects personal health information from another branch, this collection is considered a use of the information by the Department. Branches may only collect personal health information from other branches within the Department in accordance with POLICY V: Use of Personal Health Information.

Notice of Collection

When branches collect personal health information directly from an individual, they must provide the following verbally or by way of a statement on a form:

- identify the primary purpose(s) or program function(s) for which the information is collected, and
- identify the business address and telephone number of an employee who can answer the individual's questions about the department's information collection practices

Branches are responsible for ensuring individuals receive this information. Branches may wish to contact the Legislative Unit for assistance in drafting notice statements.

Branch Lists

Branches must maintain listings of the personal health information they collect. These lists must indicate the purpose for the collection and whether the information is collected directly or indirectly from the individual.

Branches must review these lists annually to determine if the personal health information they collect is still necessary.

Duty to Ensure Accuracy

Branches must take reasonable steps to ensure that the information they collect is accurate, up to date, complete and not misleading.

Responsibility

Branch leads are responsible for ensuring that this policy is followed.

Additional information on these responsibilities may be sought from the Legislative Unit.

Authority

The Personal Health Information Act – Sections 13, 14 and 15

Effective Date:

October 1, 2003

Revision Date:

June 1, 2017

POLICY IV: Disclosure of Personal Health Information

Policy

It is the policy of the Department, as a trustee under *The Personal Health Information Act* (PHIA), to limit disclosures of personal health information in accordance with the requirements of PHIA.

Procedure

Definition of Disclosure

For the purposes of PHIA and this policy, "disclosure" means the act of revealing personal health information to a person or organization outside the boundaries of the Department.

Providing personal health information to other government departments and agencies, regional health authorities, health care providers, and friends and family of the individual are all examples of disclosures. Providing information by mail, email, fax, phone or in person may also be examples of disclosures.

Branches should note that, even where the Department provides information to another person or organization defined as a trustee under PHIA, that act still constitutes a disclosure. Disclosures to other trustees must be authorized by PHIA and this policy.

Limitations on Disclosure of Personal Health Information

The Department will only disclose personal health information where one of the following conditions exists:

- the individual the information is about has consented to the disclosure, or
- the disclosure without consent is authorized by PHIA or another enactment of Manitoba or Canada

All consents for disclosure of personal health information must be in the form described in POLICY VI: Consent to the Use or Disclosure of Personal Health Information, unless another form approved by the branch obtaining the consent is used. This does not preclude a Branch from accepting consent submitted by a third party requesting the disclosure of information, ex: a lawyer acting for the individual the information is about or an insurance company.

Disclosure without Consent

The Department is permitted to disclose personal health information without the consent of the individual the information is about if the disclosure is:

- to a person who is providing or has provided or will be providing health care to the individual, to the extent necessary to provide health care to the individual, unless the individual has instructed the Department not to make the disclosure,
- to any person if the Department reasonably believes that the disclosure is necessary to prevent or lessen a serious and immediate threat to

    - the mental or physical health or the safety of the individual the information is about or another individual, or
    - public health or public safety
- for the purpose of
    - contacting a relative or friend of an individual who is injured, incapacitated or ill
    - assisting in identifying a deceased individual, or
    - informing the representative or a relative of a deceased individual, or any other person it is reasonable to inform in the circumstances, of the individual's death
- to a relative of a deceased individual if the Department reasonably believes that disclosure is not an unreasonable invasion of the deceased's privacy
- required for
    - the purpose of peer review by health professionals
    - the purpose of review by a standards committee established to study or evaluate health care practice in a health care facility or health services agency
    - the purpose of a body with statutory responsibility for the discipline of health professionals or for the quality or standards of professional services provided by health professionals, or
    - the purpose of risk management assessment
- to a health researcher, pursuant to an appropriate Research Agreement, and where the research has received prior approval from the Health Information Privacy Committee
- to an Information Manager, pursuant to an appropriate Information Manager Agreement
- to another trustee who requires the information to evaluate or monitor the quality of services the other trustee provides
- for the purpose of determining or verifying the individual's eligibility for a program, service or benefit, if the information disclosed is limited to the individual's demographic information
- to another trustee for the purpose of de-identifying the personal health information
- for the purpose of
    - delivering, evaluating or monitoring a program of the Department that relates to the provision of health care or payment for health care
    - for research and planning that relates to the provision of health care or payment for health care by the Department
- to a computerized health information network and database, established by the Manitoba government or government agency, the Government of Canada or of another province or territory or an agency of such a government, an organization representing one or more governments or another trustee that is a public body specified in the Personal Health Information Regulation, in which personal health information is recorded for the purpose of:
    - providing health care
    - facilitating the evaluation or the delivery, evaluation or monitoring of a program that relates to the provision of health care or payment for health care, or
    - facilitating research and planning that relates to the provision of health care or payment for health care
- to collect a debt the individual owes to the Department or another department of the Manitoba Government, if the information disclosed is limited to demographic information
- to the government, another public body, or the government of another jurisdiction or an agency of such a government, to the extent necessary to obtain payment for health care provided to the individual the personal health information is about
- to a person who requires the personal health information to carry out an audit for or provide legal services to the Department, if the Department reasonably believes that the

person will not use or disclose the personal health information for any other purpose and will take appropriate steps to protect it
- required in anticipation of or for use in a civil or quasi-judicial proceeding to which the Department/Government of Manitoba is a party
- required in anticipation of or for use in or the prosecution of an offence
- required by police to assist in locating an individual reported as being a missing person, if the information disclosed is limited to demographic information, unless law enforcement produce a record access order or an emergency demand under The Missing Persons Act
- required to comply with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of the personal health information, or with a rule of court concerning the production of the personal health information
- for the purpose of an investigation:
    - under or the enforcement of an enactment of Manitoba respecting payment for health care, or
    - or enforcement respecting a fraud relating to payment for health care
- for the purpose of complying with an arrangement or agreement entered into under an enactment of Manitoba or Canada
- authorized or required by an enactment of Manitoba or Canada

The Minister or his or her designate may disclose an individual's personal health information to the government of another jurisdiction in Canada, or an agency of such a government, without the individual's consent, if
- the individual the information is about normally resides in the other jurisdiction
- the information is about health care he or she received in Manitoba, and
- the government of the other jurisdiction requires the information for the purpose of monitoring or evaluating the extra-jurisdictional provision of health care to its residents

Minimum Amount

Even where a disclosure is authorized by PHIA, the Department must limit the disclosure to the minimum amount of information the recipient needs to know for the stated purpose.

Restrictions on Employees

An employee may only disclose personal health information where the disclosure is consistent with the employee's previously defined role and function. Branch leads will determine which employees are authorized to make disclosures.

Before making a non-consensual disclosure, an employee must confirm that statutory authorization for the disclosure exists. If uncertain, the employee will consult with his/her branch lead. If a branch lead is uncertain, he/she will consult with the Legislative Unit or seek advice from the Department's Legal Counsel.

Requests for Disclosure

The Department regularly receives requests for the disclosure of personal health information from third parties. It is recommended that these requests be submitted to the Department using the Personal Health Information Disclosure Request Form. If branches have developed their own form for this purpose, they may use that form.

If branches do accept disclosure requests not submitted using the above form or another form they have developed for this purpose, they should require that requests be made in writing on organizational letterhead (where applicable).

Branches may determine whether written requests for disclosure are required.

Where a third party requests a disclosure under the authority of an enactment of Manitoba or Canada (other than PHIA), the branch should request that evidence of this authority be included with any written request (regardless of the format of the request), unless the branch is certain that the authority does exist.

Disclosures Pursuant to Other Legislation

Before disclosing personal health information pursuant to another enactment of Manitoba or Canada, the branch should consult with the Legislative Unit.

Disclosures for Information Management

Where the Department provides a third party with access to personal health information for the purposes of processing, storing, or destroying information, or for providing information management or information technology services, the Department must enter into a written Information Manager Agreement (IMA) with the third party.

The IMA must provide for the protection of the personal health information against such risks as unauthorized access, use, disclosure, destruction, and alteration. IMAs should be drafted by, or vetted through, Legal Counsel for the Department.

Disclosure for Health Research

Before the Department discloses any personal health information to an individual or organization for the purposes of health research, (with the exception of a health research organization described below), PHIA requires that the research be approved by the provincial Health Information Privacy Committee (HIPC).

Information may be disclosed to the following health research organizations designated by the Personal Health Information Regulation as prescribed health research organizations:

- Canadian Institute for Health Information (CIHI), and
- Manitoba Centre of Health Policy at the University of Manitoba

Personal health information may be disclosed to a designated health research organization for any of the following purposes:

- analyzing the health status of the population
- identifying and describing patterns of illness
- describing and analyzing how health services are used
- analyzing the availability and adequacy of human resources required to provide health services
- measuring health system performance, or
- health system planning

Before personal health information is provided, an agreement is required to be completed with a researcher or a designated research organization. The agreement must meet the requirements of PHIA and the Personal Health Information Regulation made under PHIA.

In addition, all disclosures of personal health information to third parties for research purposes must be approved by the Information Management & Analytics Branch. This requirement applies even if HIPC has approved the disclosure. A copy of the information disclosed must be retained by the Information Management & Analytics Branch.

Bulk Disclosures

Before making bulk disclosures, even where authorized under PHIA and this policy, branches must ensure that the disclosure is made in accordance with relevant Information Management & Analytics Branch policies and procedures.

Security

The security of the personal health information must be maintained during the course of all disclosures. Refer to POLICY VIII: Security of Personal Health Information for information on security requirements.

Record of Disclosures

Branches must create and maintain a record of all disclosures of personal health information. The record of disclosure must include the following:

- the name of the individual the information is about or any other unique identifier
- a description of the information disclosed
- the person or body who was the recipient of the information
- the method of disclosure (ex: mail, fax, verbal)
- the date of the disclosure, and
- the name of the employee that made the disclosure

If branches require requests for disclosure to be submitted by third parties using the Personal Health Information Disclosure Request Form, when completely filled out, all the information that branches are required to maintain can be found in the form.

The record of disclosure is considered to be personal health information and if a request is made by an individual to access the record of disclosure they are entitled to access the record as per POLICY I: Access to Personal Health Information.

Responsibility

Branch leads are responsible for ensuring that this policy is followed.

Additional information on these responsibilities may be sought from the Legislative Unit.

In cases of bulk disclosures or disclosures for research, assistance may also be sought from the Information Management & Analytics Branch.

Authority

The Personal Health Information Act – Sections 20, 22, 23, 24, 24.1 and 25

Effective Date:

October 1, 2003

Revision Date:

May 2, 2018

POLICY V: Use of Personal Health Information

Policy

It is the policy of the Department, as a trustee under *The Personal Health Information Act* (PHIA), to limit its use of personal health information in accordance with the requirements of PHIA.

Procedure

Definition of Use

For the purposes of PHIA and this policy, "use" refers to any action taken within the boundaries of the Department that involves personal health information. The following are examples of use of personal health information:

- access to a file or database containing personal health information by Department staff;
- sharing personal health information between branches or program areas
- internal analysis, research, processing, reproduction, transmission, or transportation of personal health information, and
- any other internal action taken on the basis of personal health information

Limitations on Use of Personal Health Information

The Department is permitted to use personal health information for the purpose for which it was originally collected. This is referred to as the "primary use". Any other use other than the primary use is considered a "secondary" use.

The Department will use personal health information only for the purpose for which it was collected or received and not for any other "secondary" purpose unless:

- the secondary purpose is directly related to the primary purpose for which the personal health information was collected or received
- the individual the personal health information is about, or his or her personal representative, has consented to the use
- use of the information is necessary to prevent or lessen a serious and immediate threat:
    - to the mental or physical health or the safety of the individual the information is about or another individual, or
    - to public health or public safety
- the personal health information is used:
    - to deliver, monitor or evaluate a program that relates to the provision of health care or payment for health care by the Department
    - for research and planning that relates to the provision of health care or payment for health care by the Department
- the information is demographic information about an individual, or his or her PHIN, and is used to
    - confirm eligibility for health care or payment for health care
    - verify the accuracy of the demographic information or the PHIN, or
    - collect a debt the individual owes to the Department or the Government

- the purpose is one for which the information can be disclosed to the Department under the permitted disclosure provisions, or
- use of the information is authorized by an enactment of Manitoba or Canada

If the Department requires consent for a secondary use of personal health information, the consent must be in the form described in POLICY VI: Consent to the Use or Disclosure of Personal Health Information.

Minimum Amount

When using personal health information, the Department will limit the use to the minimum amount of information necessary to accomplish the purpose for which it is used. This requirement applies even where the use is otherwise authorized under PHIA and this policy.

Restrictions on Employees

Employees must be authorized by branches to access and use personal health information. This authorization must be based on an employee's previously defined role and function and must be necessary to that role and function.

Employees are required to limit their access to and use of personal health information to only what they need to access or use in order to perform any specific task or function that they are authorized to perform.

Employees are prohibited from using, accessing or attempting to access information without authorization. This includes, but is not limited to:

- accessing their own personal health information, and
- accessing the personal health information of a family member, friend or co-worker

Secondary Uses

All secondary uses of personal health information must be reviewed and approved by the branch lead.

Use for Internal Research

Before using personal health information for internal research purposes, branches must consult and comply with relevant Information Management & Analytics Branch policies and procedures.

Record of Uses

Branch must maintain records of the purposes for which personal health information is used, who uses it and the authority for the use under PHIA or another act of Manitoba or Canada.

Responsibility

Branch leads are responsible for ensuring that this policy is followed.

Additional information on these responsibilities may be sought from the Legislative Unit.

In cases of use for internal research purposes, assistance may also be sought from the Health Information Management Branch.

Authority

The Personal Health Information Act – Sections 20 and 21

Effective Date:

October 1, 2003

Revision Date:

June 1, 2017

POLICY VI: Consent to the Use or Disclosure of Personal Health Information

Policy

It is the policy of the Department, as a trustee under *The Personal Health Information Act* (PHIA), to obtain consent for the use and disclosure of personal health information where required by PHIA.

Procedure

Consent Requirements

Consent for the use or disclosure of personal health information must:

a) relate to the purpose of which the information is used or disclosed
b) be knowledgeable
c) be voluntary, and
d) not be obtained through misrepresentation

Consent is knowledgeable if the individual who gives it has been provided with the information that a reasonable person in the same circumstances would need in order to make a decision about the use or disclosure of the information.

When the Department requests written consent from the individual for the use or disclosure of personal health information, the Consent to Use or Disclose Personal Health Information Form must be used, unless another form approved by the branch obtaining the consent is used. This does not preclude a Branch from accepting consent submitted by a third party requesting the disclosure of information, ex: a lawyer acting for the individual the information is about or an insurance company.

Refer to POLICY IV: Disclosure of Personal Health Information and POLICY V: Use of Personal Health Information to determine when consent is required.

Who May Provide Consent

Consent to the use or disclosure of personal health information may only be provided by the individual the information is about, or by his or her representative.

Form of Consent

Consent may be provided in writing or verbally. However, written consent is the recommended form of consent.

The Consent to Use or Disclose Personal Health Information Form is to be used except in the circumstances noted above.

A written consent must include the following information:

- the name of the person or organization that will use or receive the information
- a description of the information to be used or disclosed
- a description of the purpose for the use or disclosure
- the date or event on which the consent expires, if applicable
- a statement that the individual may revoke or amend the consent in writing at any time before it expires
- if the person providing consent is not the individual the information is about, documentation setting out their authorization
- the signature of the individual providing authorization, and
- the date the consent was signed

Consent may be given subject to conditions, but a condition that has the effect of restricting or prohibiting a trustee from recording personal health information is not effective if the recording is required by law or by established standards of professional or institutional practices. If there are conditions, these should be specified in the written consent.

Branches may accept a verbal consent in certain circumstances. If a branch is prepared to rely on a verbal consent, it must do the following:

- take reasonable steps to verify the identity of the individual giving the consent, and
- document the consent in a record maintained by the branch

Responsibility

Branch leads are responsible for ensuring that this policy is followed.

Additional information on the elements of an appropriate consent may be sought from the Legislative Unit.

Authority

The Personal Health Information Act – Sections 19.1, 19.2, 21 and 22

Effective Date:

October 1, 2003

Revision Date:

November 5, 2014

POLICY VII: Retention and Destruction of Personal Health Information

Policy

It is the policy of the Department, as a trustee under *The Personal Health Information Act* (PHIA), to retain and destroy personal health information in accordance with the requirements of PHIA and *The Archives and Recordkeeping Act*.

Procedure

The Archives and Recordkeeping Act

The Department is statutorily bound by *The Archives and Recordkeeping Act* which sets out the rules related to the retention and destruction of all government records, including records that contain personal health information.

This Act states that all recorded personal health information regardless of physical form (ex: paper (written or typed), photographs, films and electronic records (mainframe or personal computer)) cannot be destroyed or removed from the Department unless covered by a records authority schedule that has been approved by the Provincial Archivist.

Records Authority Schedules

Records authority schedules are formal plans that identify government records, establish their retention periods, and provide for their disposition. Records authority schedules are to identify and describe all records/documents created or received by branches of the Manitoba Government. A schedule specifies the length of time records are to be kept on site and at the Records Centre. Once the specified length of time has expired, the schedule authorizes the destruction or transfer of the record to the Provincial Archives for permanent storage.

Schedules must be completed by each branch with input from the Department's Records Officer. The schedules will ultimately require the approval of the Provincial Archivist.

Employees can access the records authority schedules by contacting the departmental Records Officer.

Series of Records/Documents

Each branch will determine the purpose of a series of records or documents and the appropriate retention periods for each group on a case by case basis.

Destruction of Records

The Department will ensure that personal health information is destroyed in a manner that protects the privacy of the individual the information is about.

Any document containing personal health information must be placed in appropriate Government Records boxes for destruction. Documents containing personal health information are not to be discarded in mainstream garbage.

Staff should take measures to ensure that personal health information is reasonably protected from the sight of unauthorized persons when placed in Government Records boxes. These measures may include tearing the documents, placing them under other less confidential material, and closing the lid of the box when leaving the office.

Any series of records or documents that have reached their maximum required retention period are to be destroyed by the Provincial Archives.

When computer hardware and equipment (including servers, desktop computers, laptops, notebooks, hand-helds, fax machines and photocopiers) or portable electronic storage media (including floppy disks, magnetic tapes, CDs, DVDs, USB memory sticks and portable hard drives) on which personal health information has been recorded is being disposed of or used for another purpose, the information must be magnetically erased or overwritten in such a way that the information cannot be recovered. Consult the Department's IT Security Officer for guidance.

Responsibility

Branch leads, in conjunction with the Department's Records Officer, are responsible for ensuring that this policy is followed.

Authority

The Personal Health Information Act – Section 17
The Archives and Recordkeeping Act

Effective Date:

October 1, 2003

Revision Date:

November 5, 2014

POLICY VIII: Security of Personal Health Information

Policy:

It is the policy of the Department, as a trustee under *The Personal Health Information Act* (PHIA), to protect the confidentiality, accuracy, and integrity of personal health information at all times by adopting reasonable administrative, physical and technical security safeguards in accordance with the requirements of PHIA.

Procedure:

Definitions

For the purposes of this policy:

- "removable electronic storage media" includes magnetic tape, diskettes, CDs, DVDs, USB memory sticks and portable hard-drives
- "personal computing devices (PCs)" include desktop computers, laptops, notebooks, tablets and other similar devices, and
- "portable electronic devices (PEDs)" include laptops, notebooks, tablets, cellular telephones, pagers, PDAs, iPods and other similar devices)

Administrative Safeguards

It is the responsibility of the Department to ensure that employees, students, volunteers or other individuals participating in an unpaid work experience are informed of and orientated to PHIA and the departmental *Policies and Procedures under The Personal Health Information Act* ("The PHIA Manual"), and are aware of the consequences of breaching them. Refer to POLICY X: PHIA Orientation and Ongoing Training for information on departmental PHIA training.

Branches will ensure that all new employees and agents sign a PHIA Pledge of Confidentiality as required by POLICY X: PHIA Orientation and Ongoing Training and that the signed pledge is provided to Pay and Benefits with a copy retained in the employee's branch personnel file.

Finance and Administration will ensure that confidentiality provisions and a PHIA Pledge of Confidentiality are included in all professional services contracts where it is anticipated that contract personnel could have access to personal health information.

Branches must identify which of their employees are authorized to access personal health information. Employees may only have access to the minimum amount of information they require to fulfil their responsibilities, as per POLICY V: Use of Personal Health Information.

Physical Safeguards

Administrative Services will issue identification badges (proximity readers) as a means of employee identification. Any unrecognized individual in secure areas or in areas where personal

health information is maintained or accessible should be challenged by employees and, if necessary, reported to security.

All visitors must be registered and issued visitor passes before admitted to secure areas.

Doors with combination locks must not be left open and combinations must not be disclosed to unauthorized persons. Branches are responsible for ensuring that combinations are changed once a year, or when an employee with knowledge of the combination leaves, whichever is sooner.

Under s. 3(a) of the Personal Health Information Regulation, branches must ensure that personal health information is maintained in designated areas and subject to appropriate physical safeguards. These safeguards must be appropriate to the sensitivity of the information. Physical safeguards may include locking filing cabinets and locking office/storage room doors.

Branches must take reasonable steps to ensure that personal health information in both paper and electronic format is not left in open view when employees are away from their work areas. Personal health information must be cleared from desktops and computer screens at the end of each business day.

Documents containing personal health information discarded in Government Records boxes should be reasonably protected from the sight of unauthorized persons. This may require that the documents be torn and placed under less confidential material.

Pursuant to s. 3(d) of the Personal Health Information Regulation, portable electronic devices and removable electronic storage media that contain personal health information must be locked in a secure area when not in use.

In accordance with s. 3(c) of the Personal Health Information Regulation, branches must take reasonable precautions to protect personal health information from fire, theft, vandalism, deterioration, accidental destruction, loss, or any other hazards.

Removing Personal Health Information from the Work Site

Employees may only remove personal health information from the work site where it is necessary for the performance of the employee's duties. Branch leads will determine which employees are authorized to remove personal health information from the work site.

Under s. 2(a)(i) of the Personal Health Information Regulation, when information is removed from the work site, the employee is responsible for protecting the information at all times from unauthorized access, use, disclosure, reproduction, alteration, loss, or destruction.

Personal health information must never left unattended and in plain view of unauthorized persons. For example, if personal health information must be left in a vehicle, it must be locked in a trunk or placed in a comparable secure area where it cannot be seen from outside the vehicle. Information should be placed out of view before arriving at the location where the vehicle will be parked. Personal health information must never be left in a vehicle parked in a high risk area (ex: shopping mall parking lot) even if the information is stored out of view.

Verifying Identity

Prior to disclosing personal health information, branches must take reasonable steps to:

- confirm the identity of the individual requesting or receiving the information, and

- confirm that authorization for the disclosure exists

Where personal health information is requested over the telephone, extra measures are necessary to verify the identity of the individual requesting information. Appropriate measures are to be determined by the branch and may include:

- requesting uniquely identifying information (ex: PHIN)
- returning the individual's phone call at a verified number, or
- requiring that the request be made in writing, signed, and (if applicable) submitted on organizational letterhead

If an employee is unsure of what measures to employ to verify an individual's identity or an individual's authority to receive information, he/she should consult with the branch lead. See POLICY IV: Disclosure of Personal Health Information for more information on handling third party requests for disclosure.

Transmitting Personal Health Information

When transmitting personal health information, branches must always use the most secure data transmission method available to them.

When transmitting personal health information by **mail, interdepartmental mail or courier**, branches must take reasonable steps to ensure that the information is received and opened by the intended recipient only. Envelopes must be sealed by the sender and marked "Confidential - to be opened by addressee only" or with wording of similar intent. Where the information is particularly sensitive or revealing, branches must ensure that documents are double enveloped before sent.

Personal health information provided over the **telephone** must be limited to the minimum amount of information necessary and the identity of the requestor/receiver must be verified as described in the Verifying Identity section of this policy. No personal health information is to be left on an answering machine or voicemail unless the individual the information is about has previously consented to having information communicated in that manner.

Personal health information must only be transmitted by **facsimile** (fax) where time sensitivity is an issue and where all of the following conditions are met:

- the recipient provides assurance that the information will be received in a secure area
- to the extent possible, the recipient is available to receive the fax
- the employee sending the fax is authorized to release the information
- the employee sending the fax verifies the fax number, as entered, before pressing send, and
- where the branch determines it is appropriate, a fax cover page be included that
    1. limits or excludes the inclusion of personal health information (including demographic information), and
    2. contains a confidentiality disclaimer (see APPENDIX B: Electronic Transmission Confidentiality Notice (Sample))

Personal health information may only be transmitted by **email** where all of the following conditions are met:

- the information is encrypted or is sent over a protected computer network such as the Manitoba Provincial Data Network (PDN); A listing of domains currently supported by the PDN is provided in Appendix E

- the sender verifies the email address of the recipient, as entered, before sending
- the information is de-identified to the extent possible, and
- a confidentiality disclaimer is included in the transmission (see APPENDIX B: Electronic Transmission Confidentiality Notice (Sample)), or
- pursuant to the requirements of the Customer Service Standard Regulation under *The Accessibility for Manitobans Act*, an individual that self-identifies as being disabled, requests that information that they are authorized to obtain be sent to them by email

Branches that wish to utilize **email** to communicate with individuals about departmental programs or services may only do so where all of the following conditions are met:

- the email contains only demographic information (defined by s. 1(1) of PHIA as an individual's name, address, telephone number and email address)
- the individual the information is about, or his or her representative, provides express consent
- the branch has taken reasonable steps to inform the individual, or his or her representative, of the risks involved with email communication, and
- the branch receives sign-off from at least the ADM level

Contact the Department's IT Security Officer for encryption options acceptable to the Department.

Information from the worksite, including personal health information **must not in any circumstances** be emailed to a staff member's personal email account and/or stored on their personal computer. This practice gives rise to significant security concerns as these computers may not have appropriate security safeguards from external threats and may be accessible by unauthorized persons.

The transmission of unencrypted personal health information by email or by any other means over an unprotected computer network is not permitted because of the high risk of unintentional disclosure and unauthorized access. The Province's desktop network, also known as the "Managed Environment" is a protected computer network. If the employee is not sure whether an electronic transmission to a recipient outside the government network is adequately secure, he/she will consult with the Department's IT Security Officer.

Employees should note that very few computer networks are secure enough to protect the confidentiality of unencrypted personal health information.

Technical Safeguards

The Department does not permit the unprotected storage of personal health information in any form, including electronic and digital. Where possible, personal health information should be stored in secured areas on the Government Network. Personal health information must not be stored on the hard drive or in the local memory of PCs or PEDs unless encrypted. Contact the Department's IT Security Officer to find out more about storing personal health information on the Government Network.

Wherever possible, personal health information should not be stored on removable electronic storage media. If the storage of personal health information on such a device is necessary, it must be protected through an appropriate combination of physical, technical and administrative security safeguards. Such safeguards could include locked environments, encryption, and/or agreements with information managers and couriers. These safeguards must be appropriate to

the sensitivity of the information. Examples of protected electronic storage of information includes information stored:

- on the encrypted hard drive or local memory of a PC
- in encrypted form on an unencrypted PC hard drive or local memory
- on the hard drive of an access restricted file server stored in a physically secure area (ex: in a Data Center or Server Room)
- in encrypted form on any removable electronic storage media, or
- in a secure area with a media handling scheme that records the location and content of all media at all times

Examples of unprotected electronic storage of information include:

- on the hard drive of any PC without encryption
- on removable electronic storage media without encryption if not stored in a physically secure area, or
- on any server not located in a specifically designated physically secure area including those supported within the Cloud (One Drive, Drop Box, Google Drive, etc.)

For further clarity, whenever possible, personal health information should not be stored on a mobile storage device such as a memory stick. If the storage of personal health information on a memory stick is necessary, the device must be encrypted and must be purchased through Business Transformation & Technology (BTT) of Manitoba Growth, Enterprise & Trade. For more information about this, contact the Department's IT Security Officer.

Logon, access and authentication credentials, such as user IDs/passwords, tokens, and personal identification numbers, are not to be shared with anyone. This includes co-workers, supervisors, and maintenance/repair personnel. If temporary access is required and authorized by policy or a branch lead, the user may log into a system for the person requiring temporary access and supervise their use of the account. The authorized user is responsible for the safety of personal health information accessible to the temporarily authorized individual during this time.

User accounts to information systems containing personal health information will be assigned on a single user basis only. User IDs may only be assigned to multiple users where the system or application is capable of attributing an action to a specific individual by other means. Employees are strictly prohibited from accessing any departmental health information system using the system credentials of another user.

Branches must notify the Department's IT Security Officer as soon as practicable when:

- an individual's employment is terminated, or
- an employee's duties change and the change may affect their need to access departmental health information systems to perform their duties

User IDs, passwords, PINs, door codes and other credentials must be kept confidential (ex: to avoid disclosing them to anyone or writing them down) and changed immediately if potentially compromised.

All personal computer monitors, upon which personal health information is displayed, must have screen saver passwords that activate after no more than 20 minutes of inactivity.

All passwords to electronic information systems containing personal health information are to be changed on a regular basis, but not less often than every 90 days.

All employees must log out of the computer system at the end of each business day.

Under section 5 of the Personal Health Information Regulation, branches are required to review all health information system users annually to ensure that employees have been granted access to systems only if and to the extent required to perform their duties.

Monitoring Electronic Access

Section 4(1) of the Personal Health Information Regulation requires the Department to create and maintain, or have created and maintained, a record of user activity for any electronic information system it uses to maintain personal health information. Under s. 4(4), the Regulation further requires the Department to audit records of user activity to detect security breaches, in accordance with guidelines set by the minister. For more information, see POLICY XI: Record of User Activity.

General Security Requirements

Employees shall not make any attempt to circumvent, disable, or otherwise avoid any security safeguard established under this policy and in accordance with PHIA.

Security Audits

Branches must conduct a review of the security safeguards required by this policy every two years.

Responsibility:

All employees are responsible for ensuring that the information they use in the course of their duties is maintained in a safe and secure manner in accordance with PHIA and this policy.

Branch leads are ultimately responsible for the security of the personal health information maintained within their area.

Additional information on these responsibilities may be sought from the Legislative Unit.

Branches may consult with the Legislative Unit for more information on administrative security matters and with the Department's IT Security Officer for more information on electronic security matters.

Authority

The Personal Health Information Act – Sections 18 and 19
Personal Health Information Regulation

Effective Date:

October 1, 2003

Revision Date:

May 2, 2018

POLICY IX: Corrective Procedures to Address Security Breaches Involving Personal Health Information

Policy:

It is the policy of the Department as a trustee under *The Personal Health Information Act* (PHIA), to address complaints and conduct investigations related to security breaches involving personal health information (PHI) in accordance with the requirements of PHIA and the Personal Health Information Regulation.

Procedure:

Definitions

For the purposes of this policy:

- "Agent" means a contracted person, volunteer, student, researcher, educator, member of a Board or Committee, Information Manager, or agent of any of the foregoing
- "Health Information System" means any electronic information system created and maintained by the Department that contains personal health information and to which access is provided to other trustees, and includes, but is not limited to:
    - Drug Program Information Network (DPIN including DPIN HIST)
    - Insurance Registry (IREG)
    - Manitoba Immunization Monitoring System (MIMS)
    - Claims Processing System (CPS)
- "Security Breach" has occurred if the integrity or security of personal health information collected and maintained by the Department is compromised
- "Privacy Breach" has occurred if personal health information collected and maintained by the Department is accessed, collected, used or disclosed without authorization in contravention of PHIA;
- a Security Breach includes a Privacy Breach;
- "Complaint" means a complaint made to the Department by an individual about the collection, access, correction, use, disclosure, protection or privacy of personal health information;
- types of Security Breaches:
    - *Type 1 (Administrative Security Breach)*: A Security Breach that occurs when personal health information is accessed, used or disclosed unintentionally or carelessly, without malicious intent, in contravention of PHIA, and is a result of the lack of proper policy or procedural development, or a result of failing to follow correct policy and procedure. This can include:
        i. disclosing personal health information over the phone without confirming the identity of the caller
        ii. failing to sign out of a health information system, and another employee accesses the system using the wrong userID, or
        iii. failing to properly secure paper records that would prevent potential access by those who don't have authority to access the information

- *Type 2 (Internal Privacy Breach)*: A Security Breach that occurs when personal health information is accessed, used or disclosed in contravention of PHIA by an employee or agent of the Department. This can include:
    i. accessing personal health information about oneself
    ii. accessing personal health information about other persons for personal purposes, including family, co-workers, friends and others
    iii. sharing personal health information with others internally or externally who do not have authority to access or use the personal health information or when the employee or agent is not authorized to share the personal health information in accordance with the approved Departmental PHIA Policies and Procedures, or
    iv. collecting/altering/deleting personal health information without authority
- *Type 3 (External Privacy Breach)*: A Security Breach that occurs when personal health information in a Health Information System is accessed, used or disclosed by an employee or agent of another trustee in contravention of PHIA. This can include:
    i. accessing personal health information about oneself
    ii. accessing personal health information about other persons for personal purposes, including family, co-workers friends and others
    iii. sharing personal health information with others who do not have authority to access or use the information, or
    iv. collecting/altering/deleting personal health information without authority
- *Type 4 (Technical Security Breach)*: A Security Breach involving personal health information recorded and maintained on a server, a PC, a PED, or removable electronic storage media. This can include:
    i. a health information system is hacked
    ii. an employee's user account is hacked, or
    iii. a PC, PED or removable electronic storage media is lost, or unauthorized access to or disclosure from the PC, PED or media occurs

Reporting Security Breaches

If an employee or agent of the Department becomes aware of an actual or potential Security Breach under PHIA and/or this policy, he/she must:

- immediately take any practicable steps to cease or lessen the breach, and
- report the breach to their branch lead as soon as possible

Complaints

Any employee or agent of the Department who receives a Complaint about an actual or potential Security Breach shall immediately notify the branch that maintains the information in question, or shall immediately notify their branch lead, who will in turn notify the appropriate branch.

Report/Complaint Assessment

The branch will consult with the Legislative Unit to assess whether investigation of a Report/Complaint is warranted. In determining whether to proceed with an investigation, the following shall be considered:

- if the elapsed time has made the investigation no longer practicable
- whether the Report/Complaint has been made in good faith, and
- whether the circumstances warrant an investigation

Where it is determined that no investigation is warranted, if the assessment was done based on a Complaint filed by an individual, this individual shall be notified that no investigation will be conducted, the reason why no investigation will be conducted and, where appropriate, that they have a right to make a complaint to the Manitoba Ombudsman. Where the assessment was done based on a report filed by an employee or agent of the Department, the employee or agent shall be notified that no investigation was warranted, and where appropriate, the reason why no investigation was warranted.

Initial Investigation

Where an investigation is warranted, the branch, in collaboration with the Legislative Unit, shall conduct an initial investigation, which shall include:

- identification of the individuals involved
- identification of the personal health information in question
- the nature and extent of the alleged Security Breach
- gathering relevant documents/evidence
- consulting with the appropriate resources as required (ex: Legal Services, external trustee Privacy Officers, etc.), and
- documenting all findings and versions of the event

Based on the findings of the initial investigation, the branch, in collaboration with the Legislative Unit, shall determine the status of the event to be one of the following:

1) No Security Breach
2) Unconfirmed Security Breach, or
3) Confirmed Security Breach

Where the status of the event is determined to be Unconfirmed Security Breach or Confirmed Security Breach, the branch shall immediately inform their Assistant Deputy Minister (ADM).

No Security Breach

Where it is determined that no Security Breach occurred, if the investigation was done based on a Complaint filed by an individual, this individual shall be notified that the investigation determined no Security Breach occurred and, where appropriate, that they have a right to make a complaint to the Manitoba Ombudsman. Where the investigation was done based on a report filed by an employee or agent of the Department, the employee or agent shall be notified that the investigation determined that no Security Breach occurred.

If any notification of a potential breach has taken place, those individuals must be further notified that that the investigation determined no Security Breach occurred and, where appropriate, that they have a right to make a complaint to the Manitoba Ombudsman.

Unconfirmed Security Breach

Where the initial investigation reveals an unconfirmed Security Breach, the branch, in consultation with the Legislative Unit, must assess whether it is necessary to notify the individual(s) affected and/or the Manitoba Ombudsman to advise them of the potential breach and what steps are being taken to address it. If it is determined that some form of notification must take place, it is the responsibility of the branch lead, in consultation with the Legislative Unit, to make the notification and to document the notification, including who was notified, when they were notified, and what the details of the notification were.

If it is subsequently determined that no Security Breach has occurred, the process above must be followed.

If the unconfirmed Security Breach is subsequently determined to be a confirmed Security Breach, the process below must be followed.

Confirmed Security Breach

In compliance with s. 2(c) of the Personal Health Information Regulation, where it is determined that a Security Breach has occurred:

1) If not already done, immediate steps shall be taken to contain the Security Breach by stopping the unauthorized practice, which may include:
    - recovering personal health information
    - shutting down the system that was breached
    - revoking a user's access to a health information system (or systems), and/or
    - correcting weaknesses in physical security
2) Determine the type of security breach (see **Definitions**: Types of Security Breaches – Pg. 32). In order to meet obligations found in s. 2(b) of the Personal Health Information Regulation, the branch must:
    - for breaches of type 1, 2, and 4, fill out section 1 of the Security Breach Reporting Form and submit it to their division ADM and the Legislative Unit, or
    - for type 3 breaches, have the external organization fill out section 1 of the External Security Breach Reporting Form and submit it to their division ADM and the Legislative Unit
3) The branch, in consultation with the Legislative Unit, must assess whether it is necessary to notify the individual(s) affected and/or the Manitoba Ombudsman to advise them of the breach and what steps are being taken to address it. When assessing whether to send notification, branches should consider:
    - the nature of the breach
    - the type and sensitivity of the personal health information
    - the risk to the individual(s) if their information were used or disclosed maliciously
    - whether there is any legislated obligation to provide notification, and
    - whether there is any contractual obligation to notify partner organizations

    If it is determined that some form of notification must take place, it is the responsibility of the branch lead, in consultation with the Legislative Unit, to make the notification in a timely manner and to document the notification, including who was notified, when and how they were notified, and what the details of the notification were.

    Where it is determined that the affected individual(s) will be notified, the notification must include at minimum:
    - the personal health information that was breached, and the possible harm, if any, that could come as a result of the Security Breach, along with any suggested steps, if applicable, that the individual(s) can take to protect themselves from malicious use of their information
    - the action(s) being taken to address the Security Breach

- the contact information of someone in the Department who can answer any questions, and
- where appropriate, that they have the right to make a complaint to the Manitoba Ombudsman

Where it is determined that the Manitoba Ombudsman will be notified, the notification must be done on the Ombudsman's Privacy Breach Reporting Form. The Legislative Unit must be consulted prior to sending any information to the Manitoba Ombudsman regarding breaches, including the submission of the privacy breach reporting form, and must be copied on all correspondence to the Ombudsman regarding breaches.

Other notifications that should be considered include, but are not limited to, Legal Services, Human Resources, law enforcement and media.

4) Depending on the type of breach, the following steps must be taken:
   - *Type 1 (Administrative Security Breach)*: The branch, in consultation with the Legislative Unit, will develop and implement a plan to address the cause of the Security Breach with the intent of preventing that Security Breach, or one similar to it, from happening again, pursuant to s. 2(c) of the Personal Health Information Regulation. Such a plan may include:
     i. developing/amending branch program/service policies and/or procedures
     ii. developing/amending PHIA departmental policies and/or procedures, or
     iii. requiring PHIA training/retraining for affected employees or agents
   - *Type 2 (Internal Privacy Breach)*: The branch, in consultation with the Legislative Unit, will determine whether further investigation into the accesses to personal health information is required or warranted in order to determine 1) the full extent and severity of the current Security Breach, and 2) whether or not other additional undetected Security Breaches exist. Following this determination and any subsequent additional investigation, the following steps shall be taken:
     i. where appropriate, contact Human Resources to determine what disciplinary action, if any, may be required/appropriate, and
     ii. relevant departmental/branch PHIA policies and procedures shall be reviewed to determine whether reasonable changes can be made to a) prevent this type of Security Breach from occurring again, and b) enable this type of Security Breach to be detected sooner
   - *Type 3 (External Privacy Breach)*: The branch, in consultation with the Legislative Unit and the external trustee Privacy Officer, will determine whether further investigation into the accesses to personal health information is required or warranted in order to determine 1) the full extent and severity of the current Security Breach, and 2) whether or not other additional undetected Security Breaches exist. Following this determination and any subsequent additional investigation, the following steps shall be taken:
     i. the external trustee will advise the branch of any action taken to address the Security Breach

ii. relevant departmental/branch PHIA policies and procedures shall be reviewed to determine whether reasonable changes can be made to a) prevent this type of Security Breach from occurring again, and b) enable this type of Security Breach to be detected sooner
iii. the branch shall ensure that the external trustee reviews its relevant PHIA policies and procedures to determine whether reasonable changes can be made to a) prevent this type of Security Breach from occurring again, and b) enable this type of Security Breach to be detected sooner, and the trustee will advise the branch of its findings of the review and of any steps taken as a result of the findings of the review, and
iv. the external trustee shall take any other action required by the branch to address the Security Breach

- *Type 4 (Technical Security Breach)*: The branch, in collaboration with the Information Services Branch, shall determine:
  i. the extent of the Security Breach, including the health information system(s) involved and the personal health information in question
  ii. the cause of the Security Breach, and
  iii. the corrective measures required to address the Security Breach

To assist branches in the breach management process, the following breach management checklists have been developed to guide the branch though the steps required by this policy:

- Breach Management Checklist – Type 1
- Breach Management Checklist – Type 2
- Breach Management Checklist – Type 3
- Breach Management Checklist – Type 4

Final Notification

If notification was previously sent to the individual(s) affected, the branch, in consultation with the Legislative Unit, must send a final notification to the individual(s) affected outlining:

- the findings of the investigation, including the details of the Security Breach
- the action(s) taken to address the Security Breach
- the action(s) taken to reduce the risk of a similar Security Breach occurring again
- the contact information of someone in the Department who can answer any questions, and
- where appropriate, that they have the right to make a complaint to the Manitoba Ombudsman

If notification was previously sent to the Manitoba Ombudsman, the branch, in consultation with the Legislative Unit, must send a final notification to the Manitoba Ombudsman outlining:

- the findings of the investigation, including the details of the Security Breach
- the action(s) taken to address the Security Breach
- the action(s) taken to reduce the risk of a similar Security Breach occurring again, and
- whether any notification occurred, including the details of any notification made

Final notification to any other person or organization previously notified must also be considered.

Documentation

The branch must complete, or in the case of an external security breach, have the external organization complete, Section 2 of the relevant security breach reporting form for all confirmed Security Breaches and provide a copy to the Legislative Unit, which is responsible for, in coordination with the branch, reviewing and making recommendations for measures to prevent future Security Breaches. This is to meet recording obligations in s. 2(b) of the Personal Health Information Regulation.

All security breach documents are located on the departmental intranet at http://health.intranet.mbgov.ca/phia/policies.htm.

Reporting

The branch will be responsible for providing the Assistant Deputy Minister with the findings of the investigation and a copy of the completed breach reporting form.

The Legislative Unit shall produce an annual Security Breach summary report for the Department.

Responsibility:

Branch leads are ultimately responsible for reporting Security Breaches to their ADM and the Legislative Unit and for ensuring that investigations are conducted where appropriate and in a timely manner within their area.

Branch leads are responsible for ensuring that notifications are made in a timely manner when it is determined that such notifications are required.

Additional information on these responsibilities may be sought from the Legislative Unit.

Authority

Personal Health Information Regulation – Sections 2(b) and 2(c)

Effective Date:

November 5, 2014

Revision Date:

June 1, 2017

POLICY X: PHIA Orientation and Ongoing Training

Policy:

It is the policy of the Department, as a trustee under *The Personal Health Information Act* (PHIA), to provide orientation and ongoing training for its employees and agents about PHIA and the Department's PHIA-related security policies and procedures in accordance with the requirements of the Personal Health Information Regulation.

Procedure:

Background

Unauthorized use or disclosure of personal health information is a contravention of PHIA for which an employee could be disciplined and, depending on the circumstances, even charged with an offence under the Act. The Department has an obligation to take reasonable steps to ensure that all employees are aware that they have specific obligations under PHIA to protect the privacy of personal health information and that they are aware of the potential consequences of failing to comply with those obligations.

Orientation and Ongoing Training

Pursuant to s. 6 of the Personal Health Information Regulation, branches shall ensure that new employees and agents complete the departmental PHIA Online Training Course available through Organizational Staff Development (OSD) within 5 working days of beginning employment. Seasoned employees who have completed the above full online course are required to complete the PHIA Refresher Course version at minimum every three years. Branches where employees and agents have access to a greater amount or sensitivity of personal health information should consider requiring more frequent refresher courses.

The full online training course is a pre-requisite for the refresher course.

Upon completion of either course, a certificate of course completion will be made available, which must be printed off and provided to the employee's immediate supervisor. Branches are required to maintain these certificates with the employee's signed PHIA Pledge of Confidentiality.

PHIA Pledge of Confidentiality

Pursuant to s. 7 of the Personal Health Information Regulation, the Department is required to ensure that each employee and agent signs a pledge of confidentiality that includes an acknowledgment that he or she is bound by the Department's PHIA-related security policies and procedures and is aware of the consequences of breaching them.

On the first day of work, or as soon thereafter as reasonably possible, and prior to being given access to any departmental electronic health information system in which personal health information is maintained, branches shall ensure that a new employee or agent signs a PHIA Pledge of Confidentiality and that:

1. the original is sent to Human Resources, and
2. a copy is maintained by the Branch

A PHIA Pledge of Confidentiality must be re-signed in the following circumstances:

- when there is an increase in the amount or sensitivity of personal health information that an employee has access to, or
- subject to other disciplinary action that may be determined on a case-by-case basis, when an employee has contravened PHIA or any departmental PHIA policy or procedure

Branches shall consult with the Legislative Unit when assessing whether or not PHIA or any departmental policy or procedure has been contravened.

Employees that have questions about their obligations under PHIA prior to signing the PHIA Pledge of Confidentiality can contact the Legislative Unit to discuss their questions.

Finance and Administration will ensure that confidentiality provisions and a PHIA Pledge of Confidentiality are included in all professional services contracts where it is anticipated that contract personnel could have access to personal health information.

Tracking and Reporting

The Legislative Unit will ensure that employee PHIA training course participation is tracked. Reports will be submitted to division ADMs quarterly so that employee attendance can be monitored and verified by branches under their direction.

The Legislative Unit shall produce an annual PHIA training statistical summary report for the Department.

Responsibility:

Branch leads are ultimately responsible for ensuring that their employees and agents complete PHIA training and sign or re-sign PHIA pledges of confidentiality as required by this policy.

Authority

Personal Health Information Regulation – Sections 6 and 7

Effective Date:

November 5, 2014

Revision Date:

May 2, 2018

POLICY XI: Records of User Activity (RoUA)

Policy:

It is the policy of the Department, as a trustee under *The Personal Health Information Act* (PHIA), that all branches/units create and maintain, or have created and maintained, a record of user activity for any electronic information system it uses to maintain personal health information, and to audit records of user activity to detect security breaches, in accordance with the Guidelines for Records of User Activity (RoUA).

Procedure:

Background

Every use and disclosure by a trustee of personal health information must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used or disclosed. Furthermore, it is an offence for an employee, officer or agent of a trustee to use, gain access or attempt to gain access personal health information without authorization. The Department, as a trustee under PHIA, is required by s. 4(4) of the Personal Health Information Regulation to audit records of user activity to detect unauthorized accesses, in accordance with guidelines set by the minister.

Definition

For the purposes of this policy:

- "Record of User Activity (RoUA)" means a record about access to personal health information maintained on an electronic information system, which identifies the following:
    - individuals whose personal health information has been accessed
    - persons who accessed personal health information
    - when personal health information was accessed
    - the electronic information system or component of the system in which personal health information was accessed, and
    - whether personal health information that has been accessed is subsequently disclosed under section 22 of the Act

Ensuring Logging Capability

Before a new system is implemented, the program area responsible for the new system, in consultation with the Information Systems Branch, must ensure that the system has the ability to:

1. produce an electronic record of every successful or unsuccessful attempt to
    a. gain access to the personal health information maintained on the system, and
    b. add to, delete, or modify the personal health information maintained on the system, and

2. record every transmission of personal health information maintained on the system

Record not Required

As per s. 4(3) of the Personal Health Information Regulation, in the following circumstances, a record of user activity is not required:

(a) if personal health information is demographic or eligibility information listed in Schedule B of the Regulation (see below), or is information that qualifies or further describes information listed in Schedule B of the Regulation

(b) if personal health information is disclosed under the authority of clause 22(2)(h) of the Act (disclosure to a computerized health information network) in a routine and documented transmission from one electronic information system to another

(c) if personal health information is accessed or disclosed while a Trustee is generating, distributing or receiving a statistical report, as long as the Trustee

(i) maintains a record of the persons authorized to generate, distribute and receive such reports, and

(ii) regularly reviews the authorizations

Schedule B: Demographic and Eligibility Information

- Name
- Signature
- Address
- Telecommunications information
- Sex
- Date of birth
- Date of death
- Family associations
- Eligibility for health care coverage
- Jurisdiction of residence
- Manitoba Health Registration Number
- Personal Health Identification Number(PHIN)
- A unique identifier equivalent to the PHIN assigned by another Jurisdiction that pays for health care
- A unique identifier — not including a social insurance number or, except as provided in this Schedule, any other pre-existing identifier — assigned to an individual by a Trustee for its own purposes, when accessed by any Trustee
- A non-Canadian unique health identification number

Creating and Auditing Records of User Activity

Pursuant to s. 4(1) and s. 4(4) of the Personal Health Information Regulation, branches that are responsible for a health information system that maintains personal health information must create and maintain, or have created and maintained, a record of user activity for each electronic information system it uses to maintain personal health information, and in consultation with the Legislative Unit, must establish a procedure for conducting audits of records of user activity to detect security breaches in accordance with the Guidelines for Records of User Activity (RoUA).

Branches must maintain a record of user activity for at least three years.

Exempt Systems

Legacy systems (ex: systems that were in place or being implemented prior to December 12, 2000) are exempt from the requirement to create and maintain a record of user activity if they lack the functionality to do so, until such time as the system is replaced.

Branches will work towards becoming compliant when considering an upgrade of any non-compliant legacy system.

Responsibility:

Branch leads are ultimately responsible for ensuring that systems that maintain personal health information can create records of user activity (if required), and that these records are audited in accordance with the guidelines set by the minister.

Authority

The Personal Health Information Act – Section 18(3)
Personal Health Information Regulation – Section 4
Guidelines for Records of User Activity

Effective Date:

November 5, 2014

Revision Date:

November 5, 2014

POLICY XII: Annual PHIA Policy Compliance Review

Policy:

It is the policy of the Department as a trustee under *The Personal Health Information Act* (PHIA) that all branches/units review the requirements of The PHIA Manual on an annual basis to ensure that they are in compliance with the requirements of PHIA, the Personal Health Information Regulation and the Department's own PHIA security policies and procedures.

Procedure:

Background

The Department, as a trustee under *The Personal Health Information Act* (PHIA), is required by the Act to develop policies and procedures in order to ensure it complies with the Act. These policies and procedures are contained within this PHIA policy compendium, and many of them require branches/units to take certain actions on a specific basis to ensure that they are complying with these policies.

Annual Review

In order to monitor their compliance with PHIA, the Personal Health Information Regulation and departmental PHIA policies and procedures, branches/units are required to complete a PHIA Policy Compliance Review Checklist and submit it to the Legislative Unit by the end of each fiscal year. If the checklist identifies deficiencies in a branch's/unit's compliance with departmental policy, that branch/unit shall take steps to correct the deficiencies as soon as practicable, as per s. 8(1) of the Personal Health Information Regulation.

Responsibility:

Branch leads are ultimately responsible for ensuring that the PHIA Policy Compliance Review Checklist is completed and submitted to the Legislative Unit by the end of each fiscal year.

Branch leads and division leads are ultimately responsible for ensuring that any deficiencies identified in an annual review are corrected as soon as is practicable.

Authority

Personal Health Information Regulation – Sections 8(1) and 8(2)

Effective Date:

November 5, 2014

Revision Date:

June 1, 2017

APPENDIX A: Access Fee Schedule

As set out in the Access and Privacy Regulation under *The Freedom of Information and Protection of Privacy Act* (FIPPA):

Search and preparation fees
4(1) An applicant shall pay a search and preparation fee to the public body whenever the public body estimates that search and preparation related to the application will take more than two hours.

(2) The fee payable for search and preparation is $15.00 for each half-hour in excess of two hours.

(3) When calculating search and preparation time, a public body shall include time spent in severing any relevant record under subsection 7(2) of the Act, but shall not include time spent

(a) in connection with transferring an application to another public body under section 16 of the Act
(b) preparing an estimate of fees under section 7
(c) reviewing any relevant record to determine whether any of the exceptions to disclosure apply, prior to any severing of the record
(d) copying a record supplied to the applicant; or
(e) preparing an explanation of a record under subsection 14(2) of the Act.

Copying fees
5(1) An applicant who is given a copy of a record shall pay the following copying fees to the public body:

(a) 20 cents for each page for paper copies made by a photocopier or computer printer
(b) 50 cents for each page for paper copies made from a micro printer
(c) actual costs for any other method of providing copies.

5(2) Despite subsection (1), an applicant requesting copies of his or her own personal information is not required to pay a copying fee if the total copying fee payable is less than $10.00.

Computer programming and data processing fees
6 When a public body needs to the use computer programming or incurs data processing costs in responding to an application, the applicant shall pay to the public body

(a) $10.00 for each fifteen minutes of internal programming or data processing; or
(b) the actual cost of external programming or data processing incurred by the public body.

APPENDIX B: Electronic Transmission Confidentiality Notice (Sample)

The information accompanying this transmission is intended for a specific individual and purpose. The information is private, and is protected by law. If you are not the intended recipient, you are hereby notified that any use, disclosure, copying or distribution of this information is strictly prohibited. If you have received this transmission in error, please notify us immediately by telephone. If you have received this transmission in electronic form, please destroy any record of it. If you received this transmission in paper form, please return the original to us by regular mail. Thank you.

APPENDIX C: PHIA Policy Compliance Review Checklist

The PHIA Manual sets out the following requirements for all departmental branches/units.

Departmental Policy Requirement	Frequency	In Compliance		
		Yes	No	N/A
Branches must maintain a tracking log of requests for access under PHIA and responses. (POLICY I: Pg.7)	Ongoing	☐	☐	☐
Branches must maintain listings of the personal health information they collect. These lists must indicate the purpose for the collection and whether the information is collected directly or indirectly from the individual.	Ongoing	☐	☐	☐
Branches must review these lists annually to determine if the personal health information they collect is still necessary. (POLICY III: Pg.13)	Annually	☐	☐	☐
Branches must create and maintain a record of all disclosures of personal health information. (POLICY IV: Pg.18)	Ongoing	☐	☐	☐
Branches must maintain records of the purposes for which personal health information is used, who uses it and the authority for the use under PHIA or another act of Manitoba or Canada. (POLICY V: Pg.20)	Ongoing	☐	☐	☐
Branches are responsible for ensuring that combinations are changed once a year, or when an employee with knowledge of the combination leaves, whichever is sooner. (POLICY VIII: Pg.27)	Annually	☐	☐	☐
Branches that are responsible for an electronic health information system that maintains personal health information must create and maintain, or have created and maintained, a record of user activity for each electronic information system it uses to maintain personal health information. (POLICY XI: Pg.41)	Ongoing	☐	☐	☐
In consultation with the Legislative Unit, branches must establish a procedure for conducting audits of the records of user activity to detect security breaches in accordance with the Guidelines for Records of User Activity (RoUA). (POLICY XI: Pg.41)	Ongoing	☐	☐	☐

Departmental Policy Requirement	Frequency	In Compliance		
		Yes	No	N/A
Branches are required to review all health information system users annually to ensure that employees have been granted access to systems only if and to the extent required to perform their duties. (POLICY VIII: Pg.30)	Annually	☐	☐	☐
Branches must conduct a review of the security safeguards required by POLICY VIII: Security of Personal Health Information every two years. (POLICY VIII: Pg.31)		Last completed: _____		
• All branch/unit employees, students, volunteers or other individuals participating in an unpaid work experience have completed a PHIA orientation or ongoing training session or course within the last two years.		☐	☐	☐
• All branch/unit employees, students, volunteers or other individuals participating in an unpaid work experience have signed a PHIA Pledge of Confidentiality.		☐	☐	☐
• Branches must ensure that personal health information is maintained in designated areas subject to reasonable physical safeguards.		☐	☐	☐
• Portable electronic devices and removable electronic storage media that contain personal health information must be protected through an appropriate combination of physical, technical and administrative security safeguards.		☐	☐	☐
• Branches must take reasonable precautions to protect personal health information from fire, theft, vandalism, deterioration, accidental destruction, loss, or any other hazards.		☐	☐	☐
• Branches must ensure that personal health information is disclosed by phone, mail, interdepartmental mail, courier, fax and email in accordance with departmental policy.		☐	☐	☐

Deficiencies identified? ☐ Yes ☐ No

If yes, date to be addressed by: _____

Signoff:

_____ _____

Authorized Person (print name) Branch/Unit

_____ _____

Signature Date

For more information, contact the Legislative Unit at (204) 788-6612.

APPENDIX D: PHIA Document/Form Download List

Breach Management Checklist – Type 1

Breach Management Checklist – Type 2

Breach Management Checklist – Type 3

Breach Management Checklist – Type 4

Consent to Use or Disclose Personal Health Information Form

Consent to Use or Disclose Personal Health Information Form (FR)

External Security Breach Reporting Form

Guidelines for Records of User Activity (RoUA)

Personal Health Information Access Request Form

Personal Health Information Access Request Form (FR)

Personal Health Information Correction Request Form

Personal Health Information Correction Request Form (FR)

Personal Health Information Disclosure Request Form

Personal Health Information Disclosure Request Form (FR)

PHIA Pledge of Confidentiality

PHIA Policy Compliance Review Checklist

Record of User Activity Request Form

Record of User Activity Request Form (FR)

Security Breach Reporting Form (Internal)

APPENDIX E: Domains Supported by the PDN

The following is a list of regional health authority domains currently supported by the Manitoba Provincial Data Network (PDN). Personal health information can be emailed to these domains without additional encryption required, in addition to the GoM domain (gov.mb.ca).

Winnipeg Regional Health Authority

manitoba-ehealth.ca
womenshealthclinic.org
calvaryplace.mb.ca
ccsmanitoba.ca
concordiahospital.mb.ca
deerlodge.mb.ca
dsmanitoba.ca
ggh.mb.ca
matc.ca
panamclinic.com
rham.mb.ca
sbgh.mb.ca
sogh.mb.ca
vgh.mb.ca
wrha.mb.ca
list.wrha.mb.ca
wrhalogistics.mb.ca
misericordia.mb.ca
rhc.mb.ca
rhcf.mb.ca
cjrg.ca
mdc-dlc.ca
manitobahospice.mb.ca
SignUpForLife.ca
wrha-ch.ca
hsc.mb.ca
exchange.hsc.mb.ca
churchillrha.mb.ca
nrha.ca
norwestcoop.ca
norwesthealth.ca
normanrha.mb.ca
santeenfrancais.com
mbtelehealth.ca
manitoba-physicians.ca
orthoinno.com
cancercare.mb.ca
healthcareersmanitoba.ca
palliativemanitoba.ca
stresshacks.ca

Prairie Mountain Health

pmh-mb.ca
brhcfoundation.ca

Northern Health (MeH hosted)

NRHA.ca

CancerCare Manitoba (MeH hosted)

cancercare.mb.ca

Southern Health- Santé Sud

southernhealth.ca
rha-central.mb.ca
sehealth.mb.ca
taborhome.ca
edenhealth.mb.ca
salemhome.ca
salemhome.net

Interlake-Eastern Regional Health Authority

Ierha.ca
Irha.mb.ca

APPENDIX F: Departmental Contact Information

David Langen
Information Technology Security Officer
Information Systems Branch
204-786-7143

Deborah Malazdrewicz
Executive Director
Information Management & Analytics Branch
204-786-7149

Saila Parveen
Health Information Privacy Committee Coordinator
Information Management & Analytics Branch
204-786-7204

Micheal Harding
Legislative and Policy Analyst (PHIA)
Legislative Unit
204-788-6612

Michelle Huhtala
Access and Privacy Coordinator (FIPPA)
Legislative Unit
204-786-7237

Claudie Carbonneau-Janisch
A/Records Officer
Finance and Administration Branch
204-786-7148

This page intentionally left blank.