NORTHERN HEALTH REGION

PHIA

(Personal Health Information Act)

SELF LEARNING PACKAGE

The Northern Health Region (NHR), as a Trustee, is bound by *The Personal Health Information Act* (hereinafter called PHIA). Pursuant to PHIA, the NHR is required to protect the confidentiality and privacy of its patients' and clients' personal health information. As a result, the NHR will not disclose personal health information except as may be allowed and required by PHIA.

All persons associated with the NHR must understand their obligation to ensure the confidentiality of personal, personal health and corporate information that they may acquire or become aware of through their association with the NHR. This includes the following:

- **Employees**
- **Physicians**
- **Board Members**
- **Volunteers**
- **Researchers**
- **Instructors & Students**
- **Agents**
- **Contractors**

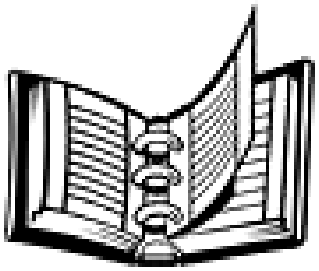
This Self Learning Package has been organized to help you understand your duties and obligations regarding the privacy and access of confidential and corporate information as it relates to your position or relationship with the NHR.

What is PHIA?

The Personal Health Information Act (PHIA) is a Manitoba Law. This Act allows individuals (patient, clients, elders) the right to examine and receive a copy of their personal health information and request a correction, protects the individual's privacy rights and establishes rules related to how personal health information is collected, used, disclosed, stored and destroyed.

We are required to protect the privacy and confidentiality of all personal health information obtained, handled, learned, heard or viewed in the course of our work or association with the Northern Health Region (NHR).

PHIA policies are found in the **Administration section (AD)** on the NHR intranet: under AD-07- Personal Health Information.



Why is PHIA needed?

Health information is personal and sensitive and its confidentiality must be protected so that individuals are not afraid to seek health care or to disclose sensitive information to health professionals.

Individuals need access to their own health information as a matter of fairness, to enable them to make informed decisions about health care and to request the correction of inaccurate or incomplete information about themselves.

A consistent approach to personal health information is necessary because many persons other than health professionals now obtain, use, and disclose personal health information in different contexts and for different purposes.

WHAT is PERSONAL HEALTH INFORMATION?

All information recorded or exchanged verbally about an identifiable individual that relates to:

- The individual's name, health or health care history, including genetic information, about the individual or the individual's family;
- What is learned or observed, including conduct or behaviour, which may be a result of illness or the effect of treatment;
- The provision of health care to the individual. Individuals include co-workers or families of co-workers when they are patients, clients, or residents of the NHR;
- Payment for health care provided to the individual

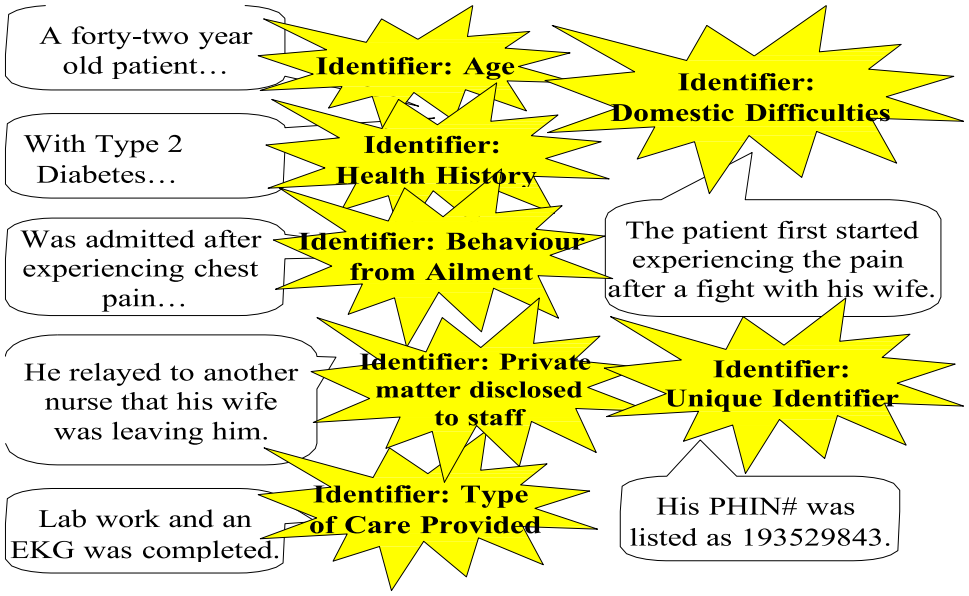
And includes

- The personal health identification number (PHIN) and any other identifying number, symbol or particular assigned to an individual, and
- 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;
- The individual's personal information, including financial position, home conditions, domestic difficulties or any other private matters relating to the individual which have been disclosed to employee or persons associated with the NHR

Demographic Information

- Means an individual's name, address, telephone number, and e-mail address.
- If the information is demographic or is his or her PHIN, it can be used to:
    - Confirm eligibility for health care or payment for health care, or
    - Verify the accuracy of the demographic information or PHIN.
- Demographic information can be used to collect a debt the individual owes to the trustee, or to the government if the trustee is a department;
- Can be used to verify the individuals eligibility for a program service or benefit, and to;
- Assist police in located an individual reported as missing as per *The Missing Persons Act.*

Examples of Personal Health Information *Identifiers*



REMEMBER: **Our patients, clients, and residents depend on us to maintain their privacy and keep their personal health information confidential.**

While you are performing your duties with the NHR, we require that you adhere to the following:

- Keep all patient, client and resident personal health information confidential and private. Do not discuss any patient, client or resident information with anyone who does not need to know this information to do his or her NHR duties.
- Do not access confidential information:
  - If the person is **not** currently in your care
  - To view your **own** information
  - To view the records of your colleagues, other employees, family, friends, neighbors, or other personal relationships (current or former)
- Access only the minimum amount of information required to do your job
- Do not share any patient, client or resident personal health or any other information provided to you;
  - in the presence of someone who does not need to know this information
  - in public places, (i.e., cafeteria, elevators, off premises).
  - on social media (i.e. Facebook, Instagram)

- You are required to ensure that all personal health information is properly secured and maintained to protect its confidentiality and is safe from accidental loss or destruction.
- All confidential material must be disposed of by an approved method (shredding).
- Anyone faxing personal health information needs to take precautions by using an approved fax cover sheet which clearly indicates that the fax contains privileged or confidential information, that unauthorized disclosure is prohibited, that the sender should be notified immediately and the original destroyed in the event that it is received by someone other than the intended recipient.
- Authorized personnel who need to transport personal health information outside the NHR premises are required to store laptops, charts, or files in the trunk of their vehicle during transportation and must never leave this information in the trunk of a vehicle in an area of high risk of theft.
- If you are not sure what is the appropriate thing to do in a specific situation, discuss it with your manager, Site Privacy Officer at your location or the Regional Privacy & Access Officer.
- Report all suspected breaches of confidentiality to your manager, Site Privacy Officer or Regional Privacy & Access Officer and complete an Occurrence Report.

Record of User Activity

The Personal Health Information Regulation requires trustees to maintain a record of user activity for any electronic information system it uses to maintain personal health information, which identifies the following:

- **individuals whose PHI has been accessed;**
- **persons who accessed it;**
- **when PHI is accessed;**
- **the electronic information system or component of the system in which PHI is accessed;**
- **whether PHI that has been accessed is subsequently disclosed under section 22 of PHIA**

Audits

PHIA requires that we run audits to detect security breaches on all electronic information systems we use to maintain personal health information. Audits could be conducted on any or all of the following triggers:

- **the user has the same last name as the individual the record is about;**
- **the user access records of co-workers, or employees from another department/facility;**
- **the user accesses their own record;**
- **a higher than normal number of users access a particular record such as a high profile name;**
- **user accesses a particular record an unusually high number of times**
- **no action was taken when a record was accessed;**
- **access was outside the user's normal working hours;**
- **access does not correspond to the user's role.**

A breach of confidentiality is when you:

- Access or request personal health information NOT NEEDED by you to do your job.
- Provide information NOT NEEDED by the other person to do their job.
- Provide information to an individual who has no right to have the information under PHIA.
- Where consent is required and consent has not been obtained from the individual or a person permitted to exercise the rights of the individual.

What is snooping?

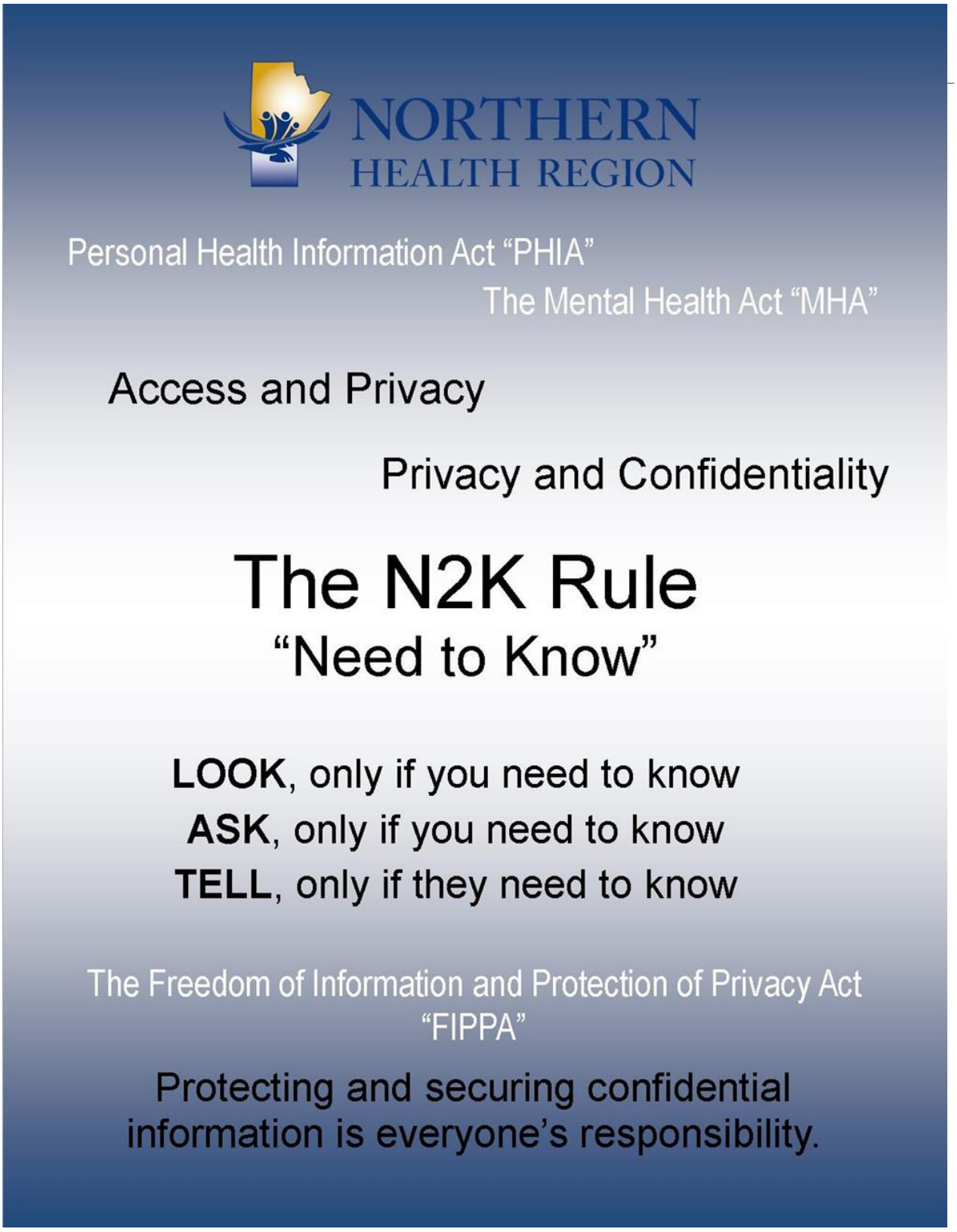
Snooping is when an employee, officer or agent of a trustee, information manager or health research organization, disregards the requirement of PHIA and willfully uses (or attempts to use) personal health information for purposes unrelated to their job duties and contrary to the Act. This includes gaining access or attempting to gain access to another person's personal health information without authorization to do so.

IF a breach of confidentiality is confirmed, discipline may include:

- Oral or written warning
- Suspension
- Termination of employment

If convicted of an offence under PHIA, the courts may fine you up to $50,000.00.

A confirmed breach of confidentiality may be reported to the individual's professional regulatory body.


NORTHERN
HEALTH REGION
Personal Health Information Act "PHIA"
The Mental Health Act "MHA"
Access and Privacy
Privacy and Confidentiality
The N2K Rule
"Need to Know"
LOOK, only if you need to know
ASK, only if you need to know
TELL, only if they need to know
The Freedom of Information and Protection of Privacy Act
"FIPPA"
Protecting and securing confidential information is everyone's responsibility.

PHIA Scenarios

The following is a compilation of scenarios with questions and answers related to them. Questions about the examples should be directed to your site Privacy Officer or designate or to the Regional Privacy & Access Officer.

EXAMPLES:

1. You are interested in some information about a family member. You ask a physician who has access to the EMR to look up the family member's information and provide you with details. The physician is not providing care to the family member. Is this a breach of confidentiality?

Yes. If the physician acted on your request, this would be a breach of confidentiality by the physician. The physician should only be accessing the records of those patients to whom they are providing care as part of their job. The physician should tell you that this is an inappropriate request. Employees caring for a patient can and do provide families with information about care currently being provided or if the patient has consented when they are providing care to the patient.

2. You may be involved in the ongoing care of an individual over the past 10 months. You are out at a social gathering and run into the daughter of the patient. She starts to ask you questions and for details about her mother's care. What should you do?

Tell her that this may not be the best time or place to have this discussion. Employees may run into family and friends of people they are providing care to in many settings outside of their workplace. These settings may include social events, grocery stores or shopping malls. As a person involved in the provision of health care you should only be discussing the people you are providing care to while in your workplace. It is not appropriate to have discussions about personal health information in public places where people who do not need to know the information may overhear.

3. Where would it be OK to discuss confidential information? In the hallway, elevator, private office, coffee shop, patient treatment areas?

In order to do your job, you may need to discuss the care and treatment of an individual in patient treatment areas such as on a unit, Emergency Department, private office, treatment room. Areas where patient care if provided. The information should be limited to the minimum amount. You should be aware of who might overhear your discussion and when possible move to a more private space. This includes cell phone conversations. If moving to a more private space is not possible, you should try to avoid providing identifying information about the patient in your discussion.

4. You work in more than one facility and have treated a certain patient at both facilities. The patient has revealed certain information at one site that they have not revealed to health care providers at the other site. You want to ensure that all health care providers involved in each facility are aware. Can you share what you know about the patient from one facility to another?

No, you cannot reveal information learned at one site to employees at the other site. If you reveal this information it could be a breach of the patient's privacy since they may not want the second site to know. You could talk to the patient and encourage them to discuss this information, if the patient chooses not to, you must respect their decision.

5. In order to do your job, you have been given access to an electronic system containing personal health information. You heard rumours that someone on your bowling team is quite ill so you decide to look up their information to see if the rumours are true. Is this a violation of confidentiality?

Yes, this is a breach of confidentiality. This is called "snooping" and is a breach of the individual's privacy. You should only be accessing the records of individual's whose care you are directly involved in. If you are not involved in the care of the individual, you should not be looking at their information.

6. You had some tests done last week and are anxious to know the results. You have access to an electronic system containing personal health information so decide to "look-up" information on yourself. Should you be doing this?

No, this is a breach of policy AD-07-135 Privacy Breach Management. As an employee, you cannot "look at" your won information without first submitting a Request to Access Personal Health Information form to the Health Information Management department to view or receive a copy of your information. You have been provided access to the electronic system to do your job. Looking at your personal health information is not part of your job and is therefore a breach of policy

7. In the course of doing your job, you see a report about a co-worker or friend who is pregnant. The report identifies the sex of the baby. You are excited and tell another co-worker or friend the sex. Is this a violation of confidentiality?

Yes, you should not be sharing information about people you know that you find out while doing your job. It is not a violation if the pregnant co-worker/friend shares this information with you and consents to the sharing it with others.

8. An employer calls the Emergency Department Monday morning and asks if a specific person was seen in Emergency over the weekend. If the employee answering the call looks at the list of individuals seen over the past 48 hours and finds no one listed with that name, what should be the response given to the employer? If the person answering the call finds the name on the list, what should be the response given to the employer?

Client consent is required. Any employees receiving a call from an employer regarding attendance in the Emergency Department should inform the caller that if they require verification of attendance, they should ask the employee to contact the Health Information Services Department and verification of attendance will be provided. A fee may be charged for this Disclosure.

9. Are we obligated to report cases of alleged child abuse?

Yes, according to The Child and Family Services Act (C.C.S.M. c. C80)

Disclosure is required under the Act according to subsection 18(1) as follows:
Subject to subsection (1.1), where a person has information that leads the person reasonably to believe that a child is or might be in need of protection as provided in section 17, the person shall forthwith report the information to an agency or to a parent or guardian of the child.

10. A co-worker needs some information quickly and tells you they can't remember their password to get into an electronic system. The co-worker asks if you could do them a favor and just log into the system and they will take over and get the information they need. What should you do?

You should never share your password with anyone. In this case, you should tell the co-worker to contact the Service Desk and get a new password. If you no longer need to be in an electronic system containing personal health information to do your job, you must log off from the system. You should never walk away from your computer without logging out or locking your system. Remember, all that you do in a system is audited and you will be held responsible.

11. You are preparing to fax a report to another health care facility. The report is for a patient being referred to a specialist for consultation. The patient's physician has discussed the consultation with the patient. There is no consent with the report. Can you send it to the specialist?

Yes you can send the fax. You do not need to get consent from the patient to disclose the information to the specialist. PHIA permits disclosure of personal health information without consent, if the information is being shared with someone who is, has, or will be providing health care to the individual.

12. A patient came into your facility today with a very unusual injury. You were involved in the care of the patient. There was lots of media coverage about the patient and injury. After work you go home and log into Facebook. Your friends immediately start asking you for details. You tell them everything you know. Is this a breach of the patient's privacy?

Yes, employees should not use social networking sites, like Facebook, to discuss personal health information of patients. This is a breach of the individual's privacy and will lead to a breach investigation that could lead to disciplinary action for the employee.

PHIA POLICIES AT A GLANCE

PHIA DEFINITIONS:

Access: the right of an individual, or a Person permitted to exercise the rights of that individual, to examine or receive a copy of the individual's personal health information maintained by the trustee.

Breach of Security: occurs whenever personal health information is collected, used, disclosed or accessed other than as authorized, or its integrity is compromised.

Confidentiality: the obligation of a trustee to protect the personal health information entrusted to it, to maintain the secrecy of the information and not misuse or wrongfully disclose it.

Confidential Information: includes, but is not limited to, personal information as defined in *The Freedom of Information and Protection of Privacy Act* (FIPPA); personal health information as defined in *The Personal Health Information Act* (PHIA); and; administrative records collected and created of the course of business of NHR and relate to legal, financial, and operational matters of a confidential nature.

Disclosure: means revealing personal health information outside the trustee, i.e. to other trustees, to family and friends of the individual or to other persons legally entitled to have personal health information released to them.

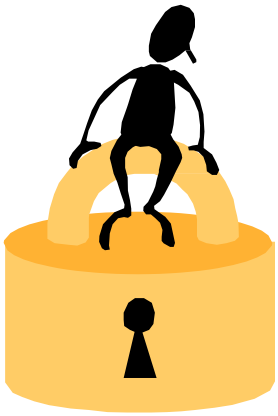
Privacy Breach: is the unauthorized access, collection, use, disclosure, or disposal of confidential information in violation of governing legislation and/or NHR.

Privacy: the fundamental right of an individual to control the collection, use, and disclosure of their personal health information.

Privacy Officer: an employee, designated by the NHR, whose responsibilities include dealing with requests from individuals who wish to examine and copy or to correct personal health information collected and maintained by the NHR, and facilitating the NHR's compliance with PHIA.

Trustee – A health professional, health care facility, public body or health services agency that collects or maintains Personal Health Information. For clarity, the NHR, as a public body, is the Trustee of Personal Health Information collected and maintained within health care facilities and sites owned and/or operated by the NHR.

Use involves revealing personal health information to someone within the trustee's own organization who needs to know the information to do their job. Use includes processing, reproduction, transmission and transportation of personal health information



Access to Personal Health Information (AD-07-115)

- Individuals have the right to examine, receive copies of, and make corrections to their personal health information.
- Requests for access to information should be in writing to the Privacy Officer or designate using AD-07-115 Appendix A, *Request for Access to Health Record* form or in a covering letter which includes the same information.
- Responding to requests for personal health information regarding ***care currently being provided:***
    - Where a request to examine personal health information is about a hospital inpatient, a member of the health care team or designate shall make the personal health information available for **examination only** within **24 hours** after receiving the request. Requested copies and explanations must be provided as soon as reasonably possible thereafter.
    - Where a request is from an individual who is **not** a hospital inpatient, a member of the health care team or designate shall make the personal health information available for **examination** and, if requested, a copy of the information must be provided to the requestor within **72 hours** after receiving the request. An explanation must be provided as soon as reasonably possible thereafter.
    - Access must be documented on the health record or on AD-07-115 Appendix A, *Request for Access to Health Record* form
    - Requests for personal health information may only be refused for reasons specified in Section 11 of *The Personal Health Information Act*.
- A response to all other requests for information must be provided within **30 days** and will be coordinated by the Site Privacy Officers or designates.
- The request for and response to requests for access to personal health information shall be included in the individual's health record.
- The provisions of *The Mental Health Act (*Manitoba) take precedence over any conflicting provisions in *The Personal Health Information Act*; refer to policy AD-07-110 Access to, Disclosure of, and Corrections to Clinical Records under the *Mental Health Act*.

Collection of Personal Health Information (AD-07-125)

- Collect only as much personal health information as needed to do your job.
- Collect information from the individual the information is about (the policy lists exceptions).
- Collect information in a manner and location that protects the confidentiality, security and integrity of that information.
- A trustee shall inform the individual of the purpose for collecting information and with whom the information will be shared. This may be done by posting notices (Your Personal Health Information, Access and Privacy in Our Facility) within the health care facility and/or providing individuals with a brochure (Health Information Access and Privacy; A Guide to The Personal Health Information Act) or verbally.

Confidentiality (AD-07-10)

- To ensure that personal health information is protected so that individuals are not afraid to seek health care or to disclose sensitive information to health professionals.
- To ensure that personal health information is protected during its collection, use, disclosure, storage, and destruction within the NHR.
- Employees are not permitted to access confidential information about themselves, their family, friends, or co-workers without following the access to information procedures set out in AD-07-115 Access to Personal Health Information.
- All employees and persons associated with the NHR shall sign a Pledge of Confidentiality The signed Pledge of Confidentiality will be filed on the individual's personnel file.
- All employees are required to complete the mandatory PHIA Absorb module.
- All employees are responsible for protecting the privacy and security of all personal health information (oral or recorded in any form) that is obtained, handled, learned, heard or viewed in the course of their work or association with the NHR.
- Use or disclosure of personal health information is acceptable **only** in the discharge of one's responsibilities and duties (including reporting duties imposed by legislation) and **based on the need to know.**
- Discussion regarding personal health information shall **not** take place in the presence of persons not entitled to such information or in public places (elevators, lobbies, cafeterias, off premises, etc.).
- Unauthorized use or disclosure of confidential information may result in disciplinary action up to and including termination.
- If you suspect a breach of confidentiality or security has occurred, immediately notify your supervisor or Privacy Officer.

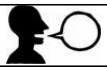
Correction of Personal Health Information (AD-07-120)

- Requests for correction of personal health information must be made in writing to the Site Privacy Officer or designate using AD-07-120 Appendix A *Request to Correct Personal Health Information* form, or in a covering letter which includes the same information.

Disclosure of Personal Health Information to Police (AD-07-50)

- In most circumstances, police are required to obtain consent for disclosure of personal health information from the individual the personal health information is about or from a person permitted to exercise the rights of that individual. If the police do not have such consent, a subpoena, warrant, or court order is required.
- Information may be disclosed to police **without consent** when the police establish that one of the exceptions applies as listed in the policy and complete AD-07-50 Appendix B *Disclosure of Personal Health Information to Police without Consent form.*
- To assist police in locating reported missing persons, the individual's **demographic information only may** be disclosed without consent. This consists of the individual's name, address, email address, and phone number.
- During normal business hours, requests for disclosure of personal health information shall be forwarded to the Site Privacy Officer or designate for processing. Requests will be reviewed to determine the urgency of the request and will be processed accordingly.
- After normal business hours, requests (with or without written consent) must be reviewed by Admin-on- Call to determine the urgency of the request. If the circumstances are urgent, copies of only the portions of the record that are required on an urgent basis should be provided. If the circumstances are not considered to be urgent, the Police should be advised to contact the Site Privacy Officer or designate in the Health Information Department on the next business day.
- The NHR is not obligated to report situations concerning individuals (i.e. discharge of individual, etc.) routinely to the Police without individual consent as outlined in the policy.
- Any reporting of persons treated for a gunshot or stab wound shall be in accordance with *The Gunshot and Stab Wounds Mandatory Reporting Act;* as outlined in policy AD-06-100, Gunshot and Stab Wounds Mandatory Reporting.
- Under *The Missing Persons Act* police may request access and/or copies of information via a Record Access Order or Emergency Demand when they have a reported missing person. They may also request access to information on a person who may be accompanying the missing person.

Use and Disclosure of Personal Health Information AD (07-70)



- Use of personal health information must be limited to the minimum amount of information necessary to accomplish the purpose for which it was collected or received.
- Use of personal health information is limited to "the need to know" for your job.
- Use is revealing personal health information to someone within the NHR.
- Disclosure is revealing personal health information to someone outside of the NHR
- Employees or persons associated with the NHR will not access their own personal health information or the health information of family or friends unless specifically requires as part of their job responsibilities and duties.
- Personal health information may be disclosed without consent of the individual, and only to the extent the recipient needs to know the information and under certain circumstances as per PHIA.
- Before using or disclosing health information, reasonable steps must be taken to ensure the information is accurate, up to date, complete and not misleading.
- Requests for use and disclosure of personal health information are coordinated with the site privacy officer or designate.

- A record of all personal health information disclosed must be kept on the health record.
- If an individual receiving health care in a health care facility or in their home and an immediate family member or someone whom the individual is known to have a close relationship asks the trustee to disclose information about current care being provided the trustee has must disclose the information as soon as reasonably possible but not later than :
    - 24 hours after receiving the request if the information is about a hospital in-patient
    - 72 hours after receiving the request, in any other cases
    - The information is about health care currently being provided
    - The disclosure is made in accordance with good medical or other professional practice
    - The trustee reasonably believes the disclosure to be acceptable to the individual
- As long as disclosure is not contrary to the express request of the individual the trustee may disclose to any person the following information about an individual who is a patient or an elder of a health care facility:
    - The individual's name
    - The individual's general health status, described as critical, poor, fair stable or satisfactory
    - The individual's location, unless disclosure of the location would reveal specific information about the physical or mental condition of the individual.
- PHIA allows for demographic information or PHIN to be used to confirm eligibility for health care or payment for health care or verifying the accuracy of the demographic information or PHIN.
- Requests for use or disclosure of personal health information must be forwarded to the Site Privacy Officer or designate.
- The individual's consent is required to disclose personal health information except under circumstances listed in this policy as per *The Personal Health Information Act*.
- Personal health information may be disclosed without consent if authorized or required to do so by an enactment of Manitoba or Canada, for example, *The Child and Family Services Act, The Fatality Inquiries Act*, *The Protection for Persons in Care Act*.

Disposal of Confidential Material, Including Personal Health Information (AD-07-20)

- Confidential material must be disposed of by shredding.

Disclosure of Personal Health Information for Legal Proceedings (AD-07-80)

- If an employee receives a subpoena they must notify their manager.
- All requests for personal health information required as part of a legal proceeding are coordinated by the Site Privacy Officer or designate or the Regional Privacy & Access Officer.
- Employees who receive a subpoena to testify are required to attend the proceeding on the required date and time.

Disclosure to Spiritual Care Providers

- Notices must be posted to inform hospital inpatients and residents of personal care homes that their names, condition, and location may be provided to a representative of their religious organization. Notices will also advise of the ability to object to the disclosure of their information. Refer to posters "Your Personal Health Information, Access and Privacy in Our Facility".
- During the admission or intake process, hospital inpatients and personal care home residents will be asked if they want their religion disclosed and will be advised that their name, condition and location may be disclosed to the specific faith group, denomination, culture, or religious organization identified by the Individual i.e. Roman Catholic, United, etc.

Privacy Breach Management (AD-07-135)

- Employees who have received a complaint about, who have knowledge of or reasonable belief that a privacy breach has occurred shall immediately notify their Manager, Site Privacy Officer, or the Regional Privacy & Access Officer and complete an Occurrence Report.
- The manager and Regional Privacy & Access Officer will consult and take immediate steps to contain the privacy breach, determine what action is required, and conduct the initial investigation.
- The manager and Regional Privacy & Access Officer will determine the status of the event.
- If a breach has been confirmed, the manager and Human Resources will consult and expand the investigation.

Reporting and Disclosure of Personal Health Information to Child and Family Services (AD-07-105)

- NHR employees, who have information that leads them to believe or suspect that a child is in need of protection, have a duty to report it.
- When the Agency is requesting personal health information the CFS worker will provide a signed and completed Manitoba Child and Family Services Personal Health Information Request Form (Appendix B).
- Disclosure of personal health information to an Agency is in accordance with *The Personal Health Information and The Child and Family Services Act.*
- All requests for disclosure of information are forwarded to the site or program that maintains the personal health information.

Retention and Destruction of Personal Health Information (AD-09-10)

- Personal health information will be retained as per retention periods outlined in the policy.

Security and Storage of Personal Health Information (AD-07-40)

- Security safeguards shall be in place to protect personal health information, i.e., locked cabinets, restricted access, security clearances, and passwords.
- Users must log off their computers when they leave the workstation.
- Computer users must not share their user IDs and passwords.
- Personal health information shall not be transmitted via e-mail outside the NHR network unless it is encrypted and password protected.
- Files containing personal health information will be kept in a designated secure storage area and not left unattended on desktops.
- Health care providers removing personal health information from the premises on authorized business shall ensure the secure storage of the information at all times.

Transmission of Personal Health Information Via Facsimile (AD-07-30)

- Use the fax cover sheet and Record of Disclosure whenever faxing personal health information as per policy.
- The sender is responsible for the security of all personal health information being sent by fax. Ensure the fax number is correct and the fax machine is located in a secure place.
- The confirmation sheet must be kept of all personal health information sent via fax.
- See *Guidelines for Faxing* (sample enclosed).

NORTHERN HEALTH REGION

RELEASE OF PERSONAL HEALTH INFORMATION
QUICK REFERENCE GUIDE

- Before disclosing personal health information, reasonable steps must be taken to ensure the information is accurate, up to date, complete and not misleading.
- Determine if there is a compelling reason to refuse disclosure as outlined in *AD-07-115 Access to Personal Health Information.*
- Information may be disclosed **only to the extent the recipient needs to know the information.**
- As long as the Trustee believes the disclosure to be acceptable to the individual or their personal representative, information about the health care **currently being provided** may be provided to an immediate family member or anyone else with whom the individual is known to have a close personal relationship within the timeframes specified in *AD-07-115 Access to Personal Health Information.*
- Unless the person has requested non-disclosure for reasons of privacy or personal safety, or the Trustee has reason to believe that the disclosure might lead to harm to the individual the information is about, the following information may be provided to any person about an individual who is a patient/resident of a health care facility:
  - Confirmation of an individual's name;
  - The location of the individual;
  - The health status of the individual described in general terms such as critical, poor, fair, stable, or satisfactory
- Individual consent **must** be obtained prior to release of information to:
  - Third party requests i.e. lawyers, MPI
  - To police. We do not automatically report situations i.e. time of discharge, etc.
- Individual consent is **not** required prior to release of information under the following circumstances
  - Continuing care i.e. transfer to another facility
  - Valid subpoenas, warrants, court orders, or court rule
  - As dictated by an Enactment of Canada or Manitoba
- Information may be disclosed to POLICE without consent under the following circumstances.
  - Any other death if so directed by the Medical Examiner;
  - Any personal health information as directed by the Medical Examiner (ME). (Confirm with the ME whether information is to be faxed directly to the ME or to the Police Agency acting as the Medical Investigator);
  - Child abuse or child in need of protection if so directed by *The Child and Family Services Act*;
  - As required by an enactment of Manitoba or Canada, such as *The Child and Family Services Act, the Protection for Persons in Care Act* or *The Criminal Code.* When disclosure is required by another Act, locate the portion of the Act that allows disclosure prior to releasing information.
  - AD-07-50 Appendix B *Request for Disclosure of Personal Health Information to Police without Consent* form must be completed by the Police indicating which of the following apply:
    - 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.
    - For the purpose of contacting a relative or friend of an individual who is injured, incapacitated, or ill.
    - For the purpose of assisting in identifying a deceased individual.
    - For the purpose of informing the representative or a relative of a deceased individual or any other person it is reasonable to inform of the individual's death.
    - To assist the police in locating an individual reported as being a missing person (**limited to demographic information only**).

GUIDELINES FOR FAXING PERSONAL HEALTH INFORMATION

BEFORE FAXING YOU MUST:

- Make sure the documents you are faxing include the fax cover sheet and Record of Disclosure
- Fax cover sheet should include;
  - Clearly identifies who is sending the fax; (Sender)
  - Clearly identifies who the fax is going to; (Recipient)
  - Records the total number of pages being faxed (including the coversheet); and
  - State the confidentiality statement.
- Double check that you have the correct fax number for the person you are sending the fax to.
- Once you have keyed in the fax number, confirm it is the correct number before pressing the "send" button.
- Set up pre-programmed fax numbers (speed dial directories) for commonly used fax numbers to avoid misdialing.
- Regularly check to ensure that speed dial fax numbers are accurate and up to date.

AFTER FAXING YOU MUST:

- Remove the documents from the fax machine – no documents containing personal health information should ever be left unattended on a fax machine.
- Check the fax confirmation sheet to make sure that all pages were successfully sent AND that they went to the correct recipient.
- Keep a copy of the fax confirmation sheet and Record of Disclosure with the original documentation that was faxed.
- When a fax contains extremely sensitive information, contact the receiver to confirm receipt.

RECEIVING FAXED DOCUMENTS:

- Remove the documents from the fax machine as soon as possible. No documents containing personal health information should ever be left unattended on a fax machine.
- Check to make sure that all pages sent to your site were received.

When personal health information is mistakenly faxed to the wrong site or person (Recipient) you MUST notify your Manager, Site Privacy Officer or Regional Privacy & Access Officer to report the breach!

Please circle the correct answer:

T	F	You have been given access to an electronic patient record so that you can do your job. It is therefore, okay for you to access anyone's information in the system as long you keep the information confidential
T	F	A piece of paper with patient names, diagnosis and treatment information is sticking out of a garbage can. Discarding these papers in the garbage can is a violation of PHIA
T	F	You work in more than one facility and have treated a certain patient at both facilities. The patient has revealed certain information at one site that they have not revealed to health care providers at the other site. You want to make sure that all heath care providers involved in each facility are aware, so you share what you know about the patient from one facility to the other. You have now breached the patient's privacy.
T	F	You received a call from an outside line in the Emergency Department asking if Miss Smith is in the ED. You can confirm that she is in the ER.
T	F	It is considered a breach of confidentiality if a client's name is released to the media without prior consent.
T	F	Employees do not have to report breaches of confidentiality to their supervisor/manager.
T	F	Consent is not needed to disclose personal health information to a lawyer
T	F	Trustees are required to audit records of user activity to detect security breaches.

Acknowledgement of Completion

I have reviewed the policy, attachments and quiz related to The Personal Health Information Act.

Employee/Student Name (Please print)	Employee #	Site/Program
Employee/Student Signature		Facilitator Signature
Date: _____		Date: _____

Please forward completed form to:

Mandy Prange
Regional Privacy & Access Officer
Northern Health Region
Email: mprange2@nrha.ca or Fax: 204-778-1408