PPG-00179

Confidentiality

Area	Access and Privacy			
Section	Protection of Privacy			
Subsection	N/A			
Document Type	Policy			
Scope	All Staff			
Approved By		**Original Effective Date**	**Revised Effective Date**	**Reviewed Date**
Penny Gilson, CEO		2016-Sep-28	N/A	N/A

DEFINITIONS

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)*; information that is collected in a clinical record as defined in *The Mental Health Act (MHA);* and; administrative records collected and created as part of the course of business and relate to legal, financial and operational matters of a confidential nature.

Information Manager: a person or body (corporation, business or association) that processes, stores or destroys personal and/or personal health information or provides information management or information technology services.

Information and Communications Technology (ICT) Resources: all assets relating to information and communications technology including, but not limited to, all information in electronic form (e.g. personal health information) and the hardware, software or network components on which information is entered, processed, stored or transmitted.

Information and Communications Technology (ICT) Services: includes all PMH internet, email, network and telecommunication services.

Personal Health Information: means information about an identifiable individual that relates to:

- the individual's health or health care history, including genetic information about the individual
- the provision of health care to the individual, or
- 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.

Personal Information: means information about an identifiable individual including:

- the individual's name
- home address, or personal phone/fax number or personal email address
- ancestry, race, colour, nationality, or national or ethnic origin
- religion or creed, or religious belief, association or activity
- blood type, fingerprints or other hereditary characteristics
- political belief, association or activity
- education, employment or occupation, or educational, employment or occupational history
- source of income or financial circumstances, activities or history
- criminal history, including regulatory offences
- involvement in legal matters.

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

Privacy Incident: an incident where the confidentiality, security, accuracy and integrity of confidential information has been compromised. A privacy incident may be accidental or as a result of intentional actions and may be as a result of operational or technical failure.

SPOT: Staff Portal for Online Training - PMH Learning Management System (LMS) which facilitates on-line registration and completion of required and voluntary education sessions.

Staff: includes all employees and persons associated with Prairie Mountain Health including: medical staff and residents, contracted individuals, students, volunteers, researchers, educators, and board members.

POLICY

Prairie Mountain Health (PMH) is committed to protecting all confidential information and adopts administrative, technical and physical safeguards to ensure the confidentiality, security, integrity and availability of this information. Confidentiality of information is governed by provincial and federal law and PMH policy.

Personal health information that is collected and maintained in a facility or a portion of a facility designated as a psychiatric facility under *The Mental Health Act (MHA)* is governed by the standards of confidentiality within this Act, which takes precedence over *PHIA* and *FIPPA.*

Staff are obligated to protect confidential information as outlined below and understand that these obligations continue after their employment/contract/association/appointment with PMH ends:

1. Staff have a legal, professional and ethical responsibility to protect all confidential information (verbal or recorded in any form) that is obtained, handled, learned, heard or viewed in the course of their work or association with PMH.

2. Confidential information must be protected and staff are responsible for using safeguards that protect the confidentiality, security and integrity and availability of this information during its collection, use, disclosure, storage, transmission, transport and destruction in accordance with applicable legislation and/or PMH policy.

3. When required to discuss confidential information, precautions are used to ensure the conversation is not overheard and is not in the presence of persons not entitled to this information such as in public places (elevators, lobbies, cafeterias, coffee shops, off premises, etc.).

4. Staff are required to use safeguards (e.g. password protection) specific to protecting the confidentiality and security of electronic information (e.g. not sharing passwords), while using ICT resources or accessing ICT services.

5. Accessing, using, disclosing or discussing confidential information is acceptable only where required in the performance of one's job duties and responsibilities and is on a "need to know" basis and only the minimum amount required. For example: Accessing, using, disclosing, or discussing an individual's information should only occur where there is a care relationship with the individual and the information is required for:
    - The provision of health care, or
    - To arrange for the provision of health care, or
    - To fulfill administrative responsibilities and duties related to supporting the provision of health-care.

6. Staff 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 PMH policy.

7. Staff who, in the performance of their duties, are required to have access to confidential information about a family member, friend or co-worker will:
    - Consult with their Manager/Supervisor to determine whether another staff member should be assigned, where possible; and
    - Where required and practical, obtain verbal consent from the client prior to fulfilling these duties.

8. All staff, as a condition of employment/contract/association/appointment with PMH, are required to complete the following prior to, or as soon a reasonably possible following, the commencement of their employment or association with PMH:
    - Confidentiality and PHIA training;
    - Review the Confidentiality policy;
    - Sign the Pledge of Confidentiality (PMH492). The pledge must be signed prior to or at the commencement of relationship with PMH and prior to working any shifts.

9. Confidentiality and PHIA refresher training and re-signing the Pledge of Confidentiality (PMH492) is required every three years.

10. The re-signing of the Pledge of Confidentiality (PMH492) is required each time there is a substantial change in the staff's position; as determined by the Director/Manager responsible for the staff. (i.e. staff moves from a department with little exposure to confidential information to a department that collects or maintains large amounts of confidential information).

11. Staff may be required to attend an additional Confidentiality and PHIA Orientation and re-sign the Pledge of Confidentiality (PMH492) at the discretion of the Director/Manager and/or Privacy Officer. (i.e. disciplinary purpose).

12. Staff have a duty to report any knowledge of or reasonable belief that a privacy incident has occurred. Reporting and management of privacy incidents is in accordance with the Privacy Incidents policy (PPG-00791, in development).

Confidentiality Agreements/Contracts

1. All Information Managers are required to enter into and sign an agreement that provides for, among other things, protection of confidential information. The Access and Privacy program oversees the execution and maintenance of all Information Manager agreements.

2. All persons or agencies contracted under a Service Agreement or another Agreement with PMH, where the service would expose them to confidential information, as a condition of acceptance of the agreement, are required to sign an Agreement that provides for, among other things, protection of confidential information.

Visitors on Business

1. Visitors attending PMH facilities for business purposes that may be exposed to confidential information (e.g. touring inpatient units, third party vendors/companies, contractors/trades people) will sign an Information and Agreement for Visitors on Business form (PMH481).

Disciplinary Response

1. Failure to comply with PMH policy that results in a privacy breach involving unauthorized access, collection, use, disclosure or destruction of confidential information may result in a disciplinary response as follows:
    - Disciplinary action up to and including termination of employment/contract/ association/appointment with the region;
    - Imposition of fines pursuant to *The Personal Health Information Act* in cases where the confidential information was personal health information; and
    - Report to an associated professional regulatory body.

RESPONSIBILITIES

Chief Executive Officer or designate:
- Ensures all Board members are provided with Confidentiality and PHIA training and sign the Pledge of Confidentiality (PMH492).

Human Resources:
- Ensures the PMH Confidentiality training video is viewed during regional orientation.
- Ensures agency agreements include clauses to ensure the agency has established policy and procedures pertaining to the privacy, security, confidentiality, and access to confidential information that extend to, and are adhered to by, all employees, agents, or persons associated with the agency.

Medical Services:
- Oversees the provision of Confidentiality and PHIA training and administration of the Pledge of Confidentiality (PMH492) for all medical staff, residents, medical students and non-PMH affiliated researchers.

Medical Director of Designated PMH Psychiatric Facility/Unit or designate:
- Oversees the orientation to the Mental Health Act for staff and students carrying out work related responsibilities in designated psychiatric facilities/units in PMH.

Volunteer Services Department, where applicable, or Directors/Managers who supervise Volunteers:

- Oversees the provision of Confidentiality training and administration of the Pledge of Confidentiality (PMH492) for all volunteers.

Access and Privacy staff:

- Oversees the development, implementation and maintenance of Confidentiality and PHIA training for PMH;
- Facilitates the provision of the training and signing of the Pledge of Confidentiality (PMH492) for students (except medical students);
- Oversees the administration of Information Manager Agreements and other information-sharing agreements.

Directors/Managers or designates:

- Ensure all employees have participated in Confidentiality and PHIA training (i.e. SPOT online training) and have signed a Pledge of Confidentiality (PMH492);
- Ensure visitors attending a facility/program for business purposes and who may be exposed to confidential information review and sign an Information and Agreement for Visitors on Business form (PMH481);
- Ensure students and instructors from educational institutions have completed the required Confidentiality and PHIA training and signed the Pledge of Confidentiality (PMH492) by verifying with the student or the Access and Privacy Program;
- Ensure contracts include clauses for the protection of Confidential Information where such information may be exposed as part of the contracted or purchased service;
- Ensure contracted service providers have completed the required Confidentiality and PHIA training and the Pledge of Confidentiality (PMH492) is signed where required (excludes agency nurses);
- Ensure that staff complete refresher training every three years.

PROCEDURE

1. All Staff complete the Confidentiality and PHIA training on SPOT and sign the Pledge of Confidentiality (PMH492) as follows:

    1.1. New Employees

    1.1.1. Human Resources:

    - Ensures the PMH Confidentiality training video is viewed during regional orientation.

    1.1.2 Director/Manager or designate:

    - Provides a copy of the Confidentiality policy and the Pledge of Confidentiality (PMH492) for the employee's review and signature;
    - Maintains the signed Pledge of Confidentiality (PMH492) in the employee's Personnel file;
    - Arranges for new employees to complete the PHIA online training on SPOT as soon a reasonably practicable, but not later than two weeks after commencement of relationship with PMH;
    - Maintains a record that the employee has completed the Confidentiality and PHIA training by including the certificate of completion (from SPOT) in the employee's Personnel file or by ensuring the training and date are recorded in the Human Resources electronic information system.

    Note: Persons who have attended an orientation session in another health region in Manitoba within the past three years may be excused from completing the SPOT online PHIA training

provided that they can produce a certificate of completion showing evidence of same. Review of the Confidentiality policy and signing of the Pledge are still required.

1.1.3 Medical Director of Designated PMH Psychiatric Facility/Unit or designate:

- Ensures that new staff hired to a designated psychiatric facility/unit, or other staff or students who will be providing services in these facilities/units are orientated to the Mental Health Act.

1.2. Medical Staff/Students/Researchers – Medical Services:

- Contacts the Access and Privacy Program to arrange for medical staff, residents and students to view the PHIA online training on SPOT prior to attending PMH;
- Arranges for approved researchers (non-PMH) to complete the PHIA online training at the time of the research approval;
- Ensures the PMH Confidentiality training video is available for viewing;
- Provides a copy of the Confidentiality policy and the Pledge of Confidentiality (PMH492) for review and signature following completion of the training;
- Maintains a record of medical staff/student/researcher's completed training and the date of completion;
- Forwards all pledges signed by medical students to the Access and Privacy program.

Note: Persons who have attended an orientation session in another health region in Manitoba within the past three years may be excused from completing the SPOT online PHIA training provided that they can produce a certificate of completion showing evidence of same. Review of the Confidentiality policy and signing of the Pledge are still required.

1.3. Students and Educators of Educational Institutions

1.3.1. Access and Privacy staff:

- Makes arrangements with the education facility staff for the students and educators to complete the PHIA online training on SPOT and view the PMH Confidentiality training video prior to attending PMH for their practical experience;
- Provides a copy of the Confidentiality policy and the Pledge of Confidentiality (PMH492) for review and signature following completion of the training. Note: The Pledge is signed once per educational program;
- Provides a document (i.e. card) as proof of completion of required education and signing of pledge and remind students and educators that this proof must be carried when on site for practicum.
- Maintains the signed pledges;
- Maintains a record of students' completed training and the date completed.

1.3.2 Medical Director of Designated PMH Psychiatric Facility/Unit or designate:

- Ensures that students and educators in a designated psychiatric facility/unit, or students and educators who will be providing services in these facilities/units are orientated to the Mental Health Act.

1.4. Volunteers

1.4.1. Volunteer Services Department, where applicable or Directors/Managers:

- Provides a copy of the Confidentiality and the Personal Health Information Act (PHIA) document (PMH226), the Confidentiality policy and a Pledge of Confidentiality (PMH492) for review and signature;
- Provides an opportunity for the volunteers to view the Confidentiality training video;
- Maintains the signed pledges;
- Maintains a record of volunteer's completed training and the date completed.

1.5. Contracted Health Care Providers (where required):

1.5.1. Managers:

- Arrange for contracted providers to complete PHIA online training on SPOT and view the PMH Confidentiality training video;
- Provide a copy of the Confidentiality policy and the Pledge of Confidentiality (PMH492) for review and Signature following completion of the training;
- Forward the signed pledges to Human Resources.

1.6. Board Members

1.6.1. Executive Management staff:

- Make arrangements for board members to complete the PHIA online training on SPOT and view the Confidentiality training video;
- Provide a copy of the Confidentiality policy and the Pledge of Confidentiality (PMH492) for review and signature following completion of the training;
- Maintain the signed pledges.

1.7. Visitors on Business (e.g. touring inpatient units, third party vendors/companies, contractors/trades people)

1.7.1. Directors/Managers who are meeting with the visitor:

- Provide the Information and Agreement for Visitors on Business form (PMH481) for the visitor's review and signature;
- Forward the signed form to the Access and Privacy program.

2. Refresher training

2.1. Every three years, or sooner as deemed necessary (e.g. discipline), Directors/Managers ensure that staff:

- Complete PHIA online training on SPOT;
- Obtain a new certificate of completion and submit this to their Supervisor/Manager to be retained in the Personnel file;
- Re-sign the Pledge of Confidentiality (PMH492) and submit this to their Supervisor/Manager to be retained in the Personnel file.

3. Contracts and Agreements

3.1. Directors/Managers ensure all service contracts/agreements, where the service provided would expose them to confidential information, include, at minimum, a standard confidentiality clause to the effect:

"The Contractor (or name of the company or party with whom the agreement is being made) shall respect and maintain the privacy and confidentiality of any and all personal, personal health, or corporate information that may be learned, viewed, heard, or otherwise acquired during the association with Prairie Mountain Health. By extension, this assurance of confidentiality shall extend to all employees, agents, or persons otherwise associated with the Contractor (or name of the company or party with whom the agreement is being made)"

3.2. Where the program/facility will be entering into a contract for information management services, Directors/Managers contact the Access and Privacy program to arrange for the administration of an Information Manager's Agreement.

RELATED MATERIAL

PMH492, Pledge of Confidentiality
PMH481, Information and Agreement for Visitors on Business
PPG-00176, Practicums, Job Shadows, Work Experience and Medical Observership (R.HR.RR.657)
PPG-00791, Privacy Incidents (in development)

REFERENCES

The Personal Health Information Act
The Personal Health Information Regulations
The Mental Health Act
The Freedom of Information and Protection of Privacy Act