Health PEI Santé Î.-P.-É.

Policy and Procedures Manual

Formal Submission for Approval

PRIVACY AND PROTECTION OF PERSONAL HEALTH INFORMATION

Health PEI			POLICY & PROCEDURES
Applies To:	Health PEI physicians, staff, students and volunteers		
Monitoring:	Chief Operating Officer, Corporate Services and Pharmacare		
Date:	Effective:	May 2007	
	Next Review:	**June 26, 2021**	

Approving Authority: Executive Leadership Team

Authorized Signature: _____

Record of Decision	Approving Body:	Executive Leadership Team
	Meeting Date:	June 26, 2018

Policy and Procedures Manual

PRIVACY AND PROTECTION OF PERSONAL HEALTH INFORMATION

Health PEI			POLICY & PROCEDURES
Applies To:	Health PEI physicians, staff, students, volunteers and any person acting on behalf of Health PEI		
Monitoring:	Chief Operating Officer, Corporate Services and Pharmacare		
Approving Authority:	Executive Leadership Team		
Date:	Effective:	May 2007	
	Next Review:	**June 26, 2021**	
This is a CONTROLLED document. Any copies of this document appearing in paper form should always be checked against the electronic version prior to use.			

1.0 POLICY

1.1 Health PEI is a custodian of personal health information ("PHI") and has responsibilities to:

(a) collect, use and disclose PHI only in compliance with the *Health Information Act* or other applicable health legislation,

(b) protect PHI in its custody or control, and

(c) respect the rights of individuals related to PHI.

1.2 PHI that is collected, used and disclosed by facilities, programs and services operated by Health PEI is in the custody and control of Health PEI and not in the custody or control of individual health care providers.

1.3 Ensuring privacy and confidentiality is essential to the trust relationship between Health PEI and its patients, residents and clients and is a core component of providing safe, quality health care.

2.0 DEFINITIONS

Aggregate data:	Data about groups of individuals, averaged or added together in such a manner as to prevent the identification of individuals, that is routinely shared for external purposes. Examples of aggregate data include wait times and statistics or data published in the Annual Report.

Circle of care:	A term commonly used to refer to information sharing practices between all health care providers (HCPs) who are part of an individual's health care team. The circle of care includes HCPs involved in the delivery of health care to the individual both within and outside of Health PEI (for example, physiotherapists working in a private clinic, private nursing home staff, First Nations Health Centre nurses or community pharmacists). Members of an individual's circle of care may be identified by the individual or by the individual's health care provider in the case of a referral.
Commissioner:	The PEI Information and Privacy Commissioner, who has a duty to monitor the administration of the *Health Information Act* and authority to conduct investigations and issue orders related to privacy and the collection, use or disclosure of PHI.
Confidentiality:	The obligation to respect an individual's privacy, protect PHI and use or disclose PHI only with appropriate authorization.
Consent:	The agreement of an individual (or person authorized to act on the individual's behalf) with an action or proposed action. Consent may be implied or express, depending on the circumstances. **Implied consent** is consent that can be assumed based on the individual's actions (for example, presenting to an emergency department seeking treatment). **Express consent** is obtained through actively asking the individual for their consent and can be verbal or written.
Data matching:	As defined in the *Health Information Act*, data matching means the creation of individually identifying PHI by combining PHI, de-identified PHI or other information from two or more databases without the consent of the individuals to whom the information relates.
De-identified information:	As defined in the *Health Information Act*, PHI that has been stripped, encoded or otherwise transformed so as to ensure that the identity of the individual cannot be readily determined.
Personal health information (PHI):	As defined in the *Health Information Act*, identifying information about an individual in oral or recorded form that includes but is not limited to information related to: • the individual's physical or mental health, family history or genetic information; • the provision of health care to the individual; • a drug, device or product provided to the individual by prescription or other authorization of a health care provider; • payments or eligibility for health care; • donation of any body part or bodily substance; or • the identity of the individual's substitute decision maker or health care provider.
Privacy:	The legal right of an individual to determine when, how and to what extent they share information about themselves with others.
Privacy Impact Assessment ("PIA"):	A process to assess a system, project or program that will involve the collection, use or disclosure of PHI to identify and address any risks to individual privacy.

Staff:	Throughout this policy, the term "**staff"** is used to refer collectively to Health PEI physicians, staff, students, volunteers and any person acting on behalf of Health PEI.

3.0 PURPOSE/SCOPE

To establish rules for the collection, use and disclosure of PHI by Health PEI staff that comply with the *Health Information Act* and other applicable legislation and reflect the Canadian Standards Association's *Model Code for Protection of Personal Information*, commonly referred to as the 10 Privacy Principles.

4.0 APPLICATION

4.1 This policy applies to:

(a) all Health PEI physicians, staff, students, volunteers and any person acting on behalf of Health PEI, and

(b) all PHI in the custody or control of Health PEI.

4.2 This policy does not apply to:

(a) de-identified information or aggregate data, and

(b) personal information, as defined in the *Freedom of Information and Protection of Privacy Act*, that is not related to an individual's health or the provision of care to the individual, including employment, financial or educational history information.

5.0 PROCEDURES

5.1 Accountability

(a) The Chief Executive Officer, as corporate head of Health PEI, has overall accountability for the organization's compliance with the *Health Information Act* and the establishment of policies and practices for the collection, use, disclosure and protection of PHI.

(b) The Manager of Health Privacy and Information Access serves as Privacy Officer for Health PEI and is accountable for:

- providing advice and consultation to staff on privacy, confidentiality and the collection, use, disclosure and protection of PHI;
- promoting privacy and confidentiality awareness;
- responding to inquiries from the public about privacy policy and practices that cannot be addressed at the facility, program or service level;
- receiving and responding to requests for correction of PHI and privacy complaints;
- leading, facilitating or supporting, as appropriate, privacy breach investigations and follow up;
- liaising with Information Technology Shared Services ("ITSS") regarding the security of PHI; and
- liaising with the Commissioner on behalf of Health PEI for matters relating to the administration of the *Health Information Act*, including breach investigations and reviews of complaints about Health PEI privacy practices.

(c) Health PEI Leadership, including Directors, Managers and Supervisors, are accountable for implementing privacy policy and practices in their areas of responsibility and for ensuring their staff are aware of and/or have access to education on privacy, confidentiality and the protection of PHI.

(d) Staff are accountable to collect, use and disclose PHI **only** in accordance with this policy and to maintain confidentiality of PHI while on and off duty.

(e) Health PEI uses contractual agreements with external contractors and service providers to ensure appropriate collection, use, disclosure and protection of PHI shared with the external parties pursuant to those agreements.

5.2 **Identifying Purpose**

(a) Health PEI collects, uses and discloses PHI for the purposes of:

- providing or assisting in the provision of health care or treatment,
- planning and management of the health care system, and
- other purposes authorized by the *Health Information Act* or other applicable legislation.

5.3 **Consent**

(a) Health PEI obtains consent from individuals for collection, use or disclosure of PHI, unless the collection, use or disclosure is permitted by law without consent. The type and manner of consent may vary depending on the situation and circumstances.

(b) Implied consent can be relied upon for the collection, use and disclosure of PHI for the purposes identified in section 5.2 Identifying Purpose.

(c) Implied consent must be knowledgeable. It must be reasonable to believe that the individual knows the purpose for which their PHI will be collected, used and disclosed.

(d) Express consent from the individual is required for:

- the disclosure of PHI to a person or organization who is not a health care provider, or
- the disclosure of PHI for a non-health related purpose.

(e) Express consent may be verbal (by asking the individual and documenting that consent was provided) or written (by having the individual sign a consent form), as appropriate.

(f) Written express consent must include:

- a minimum of two (2) identifiers for the individual whose PHI is to be disclosed,
- a description of the PHI to be disclosed,
- identification of the individual or organization to whom the PHI can be disclosed,
- how long the consent is valid (maximum of 12 months recommended),
- the signature of the individual or a person authorized to consent on their behalf, and
- the process that the individual can follow to revoke or withdraw consent.

(g) Where express consent is required, staff shall accept written express consent for the disclosure of PHI provided by an external party (for example, an insurance company or law firm) if the consent meets the first five criteria listed in 5.3 (f) above. Inclusion of the process to revoke or withdraw consent is not mandatory for forms received from external parties.

(h) If an individual is unable to consent, a substitute decision maker (SDM) may give, withhold or withdraw consent on behalf of the individual with respect to the collection, use or disclosure of the individual's PHI. The following persons, in order of priority, may act as a SDM:

- a person with written authorization from the individual to provide consent;
- the individual's guardian, spouse, adult child, parent, adult sibling or adult next of kin;
- the individual's health care provider; or
- the Public Guardian.

(i) In the case of a deceased individual, the following persons, in order of priority, may act as a SDM:

- the executor or administrator of the individual's estate; or
- the individual's spouse, adult child or parent.

(j) Individuals have a legal right to refuse or withdraw consent for the collection, use or disclosure of their PHI, with limited exceptions. Consent cannot be refused or withdrawn for:

- a collection, use or disclosure for which consent is not required (examples include disclosure for the purposes of risk management, quality improvement or a peer review), or
- a collection, use or disclosure for which refusal or withdrawal of consent is prohibited (examples include disclosure to law enforcement for the purposes of an investigation under the Criminal Code and disclosure for the purposes of monitoring the prescribing, dispensing or use of certain classes of drugs).

(k) Refusal or withdrawal of consent must be in writing.

(l) If an individual refuses or withdraws consent, staff shall:

- take reasonable steps to comply;
- explain to the individual the potential impacts to the provision of health care; and
- inform other members of the individual's circle of care (who may be involved in the collection, use or disclosure of the individual's PHI) of the refusal or withdrawal.

(m) If an individual withdraws consent for the collection, use or disclosure of their PHI, the withdrawal is not retroactive and applies going forward from the date that the individual withdrew consent.

5.4 **Limiting Collection**

(a) Health PEI collects only the **minimum** amount of PHI necessary to achieve the purpose for which the PHI is collected.

(b) Staff shall collect PHI directly from the individual that the PHI is about unless direct collection is not possible under the circumstances or may result in the collection of inaccurate PHI.

5.5 **Limiting Use, Disclosure and Retention**

(a) Health PEI uses only the **minimum** amount of PHI necessary to achieve the purpose for which it is used.

(b) Staff shall use or access PHI on a need to know basis for the purposes of:

- providing health care or treatment to an individual;
- planning, delivering, monitoring or administering health programs or services;
- risk management or quality improvement;
- educating health care providers;
- obtaining payment for or processing claims for payment related to the provision of health care; or
- other uses authorized by the *Health Information Act* or other applicable health legislation.

(c) Using or accessing PHI without the need to know for the purposes of the performance of job duties, even if the PHI is not disclosed to anyone else, is a privacy breach. Examples of the need to know for the purposes of job duties would include requiring access to PHI in order to provide care or treatment to the individual, dispense a medication, develop a plan of care, investigate a complaint or complete a chart review.

(d) Staff may use and disclose PHI within an individual's circle of care on a need to know basis for the purpose of the provision of health care or treatment to the individual.

(e) Unless the individual has expressly requested that their PHI not be disclosed, staff may rely on implied consent for the use and disclosure of PHI within the individual's circle of care.

(f) Health PEI discloses only the **minimum** amount of PHI necessary to achieve the purpose for which it is disclosed.

(g) Staff may disclose PHI:

- for the purposes for which the PHI was collected;
- with the express consent of the individual, if required;
- for auditing or accreditation purposes;
- for the purposes of an investigation, inspection, subpoena, warrant or court order;
- as required by law, or;
- for other purposes authorized by the *Health Information Act* or other applicable health legislation.

(h) Health PEI may disclose PHI for authorized research purposes. Refer to the Health PEI Data Access for Research and External Purposes Policy.

(i) If PHI is disclosed without the consent of the individual, staff shall keep a record of the disclosure which will include the name of the person to whom the PHI was disclosed, the date of disclosure and a description of the PHI that was disclosed.

(j) Health PEI limits the retention of PHI and ensures good record management practices by adhering to the retention and disposition schedules created pursuant to the *Archives and Records Act*, as part of the Health PEI Recorded Information Management (RIM) Program.

5.6 **Accuracy**

(a) Health PEI takes reasonable steps to ensure that PHI in its custody is as accurate, up-to-date and complete as possible and as necessary to achieve the purpose for which the PHI is used or disclosed.

(b) Individuals have a legal right to request correction of their own PHI that they believe is inaccurate, subject to certain limitations. Refer to the Individual Access and Correction of Personal Health Information Protocol.

5.7 **Safeguards**

(a) Health PEI protects PHI in its custody using safeguards appropriate to the format in which the information is stored and the level of sensitivity of the information. Refer to the Safeguarding Personal Health Information Protocol.

(b) If PHI is lost, stolen or used or disclosed without authorization, staff shall take immediate steps to manage the privacy breach. Privacy breaches must be disclosed to the individual whose PHI was impacted and reported to the Commissioner, except where there is no impact to the individual's care or well-being. Decisions regarding disclosure to the affected individual and reporting to the Commissioner must be made in consultation with the Privacy Officer. Refer to the Privacy Breach Management Protocol.

(c) Staff shall safeguard PHI in oral form by taking reasonable steps to prevent overhearing of conversations with patients, clients or residents by other persons. Reasonable steps will vary dependent on the physical environment and the level of sensitivity of the PHI being discussed.

(d) Staff shall ensure secure destruction of PHI that prevents unauthorized access or disclosure, when the PHI has reached the end of its life cycle, in accordance with the Health PEI RIM Policy and approved retention and disposition schedules.

(e) Health PEI provides education and training to staff on privacy and the protection of PHI, including but not limited to new staff orientation, in-services, and training on appropriate use of electronic health information systems.

(f) Staff shall complete a privacy impact assessment (PIA) prior to:

- a new or significant change to the collection, use or disclosure of PHI;
- implementation of a new or significant change to an existing electronic health information system; or
- data matching.

(g) A PIA shall describe the planned program or project, specify how PHI will be collected, used or disclosed, and identify and address any risks to individual privacy. Refer to the Privacy Impact Assessment Protocol.

5.8 **Openness**

(a) Health PEI makes information about its privacy policy and practices, including the purposes for which PHI is collected, used and disclosed, available to the public through several mechanisms, including:

- posters displayed and brochures available at Health PEI operated facilities,
- the Health PEI Privacy and Your Personal Health Information webpage, and

– the inclusion of a privacy statement and contact information for the Privacy Officer, (or preferably a person within the facility, program or service who can answer privacy-related questions) on Health PEI materials as applicable, including on forms used for the collection of PHI.

(b) Staff shall be able to explain to individuals the general purpose for the collection, use and disclosure of their PHI and provide contact information for the Privacy Officer if further information is required.

5.9 **Individual Access**

(a) Health PEI responds to requests for individual access to PHI within a maximum of 30 days, unless an extension of time is permitted by the *Health Information Act*.

(b) Individuals have a legal right of access to their own PHI, including the right to receive an audit report of all staff that has accessed their electronic health record. Individuals can ask to review or receive a copy of the PHI.

(c) There are very limited circumstances in which individual access to PHI can be refused, including if knowledge of the PHI could reasonably be expected to harm the individual or another person.

(d) In most cases, individuals can request access to their PHI directly from the facility, program or service that holds the record (e.g., Health Records department of a hospital, primary care health centre, public health program site, etc.). Refer to the Individual Access and Correction of PHI Protocol.

(e) Requests for access to PHI can be referred to the Privacy Officer if refusal of access may be required or permitted by the *Health Information Act*, or if there are any questions regarding the right of access.

5.10 **Challenging Compliance**

(a) Health PEI responds to privacy complaints received from patients, clients or residents. The Privacy Officer shall review and coordinate the investigation into privacy complaints, in collaboration with Health PEI Leadership and Quality/Risk Coordinators as appropriate, and provide recommendations for follow up. Refer to the Privacy Breach Management Protocol.

(b) Health PEI informs individuals of their right to contact the Commissioner, as applicable.

6.0 MONITORING

6.1 The Chief Operating Officer ensures that this policy is reviewed every three years according to Health PEI's policy review cycle and standards.

6.2 The Privacy Officer monitors compliance with this policy and makes recommendations for revisions, as required.

7.0 REFERENCES

Related Documents

Health PEI. (2017). "Health Information Act Staff Education Toolkit." Retrieved from http://www.healthpei.ca/src/index.php3?number=1055856

Health PEI. (2018). "Privacy and Your Personal Health Information." Retrieved from https://www.princeedwardisland.ca/en/information/sante-i-p-e/privacy-and-your-personal-health-information.

Health PEI Data Access for Research and External Purposes Policy

Health PEI Disclosure of Personal Information to Law Enforcement

Health PEI Emailing, Faxing and Electronic Transmission of Personal or Sensitive Information Policy

Health PEI Individual Access and Correction of Personal Health Information Protocol

Health PEI Privacy Breach Management Protocol

Health PEI Privacy Impact Assessment Protocol

Health PEI Public Compliments and Complaints Policy

Health PEI Recorded Information Management (RIM) Policy

Health PEI Safeguarding Personal Health Information Protocol

PEI *Archives and Records Act*, RSPEI 1988, c A-19.1

PEI *Freedom of Information and Protection of Privacy Act*, RSPEI 1988, c F-15.01

PEI *Health Information Act*, RSPEI 1988, c H-1.41

References

Corporate Privacy Policy, New Brunswick Department of Health, version 2.1, June 18, 2014

Model Code for the Protection of Personal Information (CAN/*CSA*-Q830-96)

Privacy and Confidentiality of Personal Health Information Policy, Capital Health, August 2014

Privacy of Personal Health Information Policy, IWK Health Centre, June 1, 2013

Appendices

N/A

8.0 STAKEHOLDER REVIEW

Group/Committee	Dates of Review
PEI Information and Privacy Commissioner	July 2017
Health PEI Solicitor	June 2017
IM/IT Leadership Committee	July 2017
Provincial Medical Advisory Committee (PMAC)	July 2017
Provincial Nursing Leadership Committee (PNLC)	July 2017
Patient and Family Centered Care Steering Committee	July 2017
Human Resources (Executive Director)	July 2017
Quality and Patient Safety (Executive Director)	July 2017
Allied Health Leadership (Provincial Directors)	July 2017
Health PEI RIM Coordinator	April 2018

9.0 REVIEW HISTORY

Review Dates: June 2018 _____ _____

_____ _____ _____