UNIVERSITY OF TORONTO
FACULTY OF MEDICINE

Faculty of Medicine
Statement on Protection of Personal Health Information

Approved by: Faculty of Medicine Faculty Council
Date of Adoption: February 11, 2013
HUEC Review Date: May 2017

---

1. Jurisdiction:

This statement applies to all MD Program, postgraduate, graduate professional programs involving patient care, continuing education, medical radiation sciences and physician assistant health professional learners including those registered or participating in educational activities affiliated with the Faculty of Medicine at the University of Toronto. Postgraduate trainees are learners registered through the PGME office as residents (PGYs), fellows, or formal required pre-residency programs.

2. Background and Rationale:

This statement sets out requirements to ensure that Personal Health Information[1] (PHI) (in all forms, either hardcopy or digital) in our affiliated teaching sites' custody is properly protected.

- PHI is information about the health or health care of an identifiable individual. An individual is considered to be identifiable if the information outright identifies the person, or if it is reasonably foreseeable in the circumstances that the information could be used (either alone or with other information) to identify the person. Thus, whether information is PHI depends on the context of its use.
- If it is reasonably foreseeable that a person could be re-identified, then the information is considered to be PHI. From the perspective of a custodian such as a hospital, this means that a learner (who is an agent of the hospital) must not disclose the information outside the circle of care unless either the individual consents, or it is not reasonably foreseeable, within the context of the information's use, that the individual could be re-identified.
- Even where information is considered to be de-identified to the point where the patient cannot be re-identified, if context and other information known outside of the circle of care could still be used to re-identify that individual; then that de-identified information would still be considered PHI.
- Access to PHI brings special responsibilities with respect to patient privacy and supporting public confidence in our hospitals, institutions and practices.

Obligations in regard to PHI are set out in Ontario's health information privacy legislation, entitled the Personal Health Information Protection Act, 2004 (PHIPA). PHIPA requires "Health Information Custodians" (HICs) such as hospitals to take reasonable steps to ensure that PHI is protected against theft, loss and unauthorized use or disclosure, and to ensure that records containing PHI are protected against unauthorized copying, modification or

[1] As defined in the Personal Health Information Protection Act, 2004 (PHIPA) (https://www.ontario.ca/laws/statute/04p03) includes identifiable information such as name, address, identifying numbers and other unique characteristics; as well as information for which it is reasonably foreseeable in the circumstances that it could be used with other information to identify an individual.

disposal. Learners engage in patient care and education involving access to PHI through the affiliation agreements between the University of Toronto and the Hospitals and in other healthcare placements. Under PHIPA Section 37(1) (e), as agents of HICs, such as hospitals, learners are permitted to use PHI. Accordingly, learners are required to be aware of and comply with the HICs' requirements and the HICs are required to make those requirements known to learners.

Learners need access to systems containing PHI in order to provide appropriate clinical service and to fully benefit from their clinical education experience. Learners should only access PHI when doing so is relevant to patient care. Once PHI is no longer required by the learner to provide patient care within a given institution, access should no longer be granted or be made available within that institution. Use or disclosure of material that identifies patients without proper authority constitutes a breach of law and standards of professionalism, privacy and confidentiality that potentially harms patients, the learner, the profession and our organizations. This includes intentionally or unintentionally placing material that identifies patients in the public domain. It is recognized that learners may require access to PHI stored in a secure institutional environment when they are physically outside institutions or, even when mobile within institutions.

Furthermore, it is recognized that learners, being involved in both university and hospital environments, are exposed to varying perspectives on the use of information. Universities by their nature are intended to be open and collaborative where information is encouraged to be shared, and existing university based portals, learning tools or email systems allow this to occur; hospitals are intended to be confidential within the circle of care. University information systems are not designed to support the transmission and storage of PHI and therefore should not be used for this purpose.

Learners must comply with this statement in respect of all formats (including hard copy media, and any form of information technology) that could be used to store or transmit PHI. In the current context, this includes all information and communication equipment such as personal computers, portable storage, networked information and handheld devices, as well as email, text messaging, cloud services, software applications, as well as mobile device applications and or social networking tools.[2]

This statement was developed to provide guidance for the protection of PHI in the context of the HIC as a learning environment.

3. Guiding Principles:

This statement is based on the following foundational principles:

a) Learners need access to PHI to fully benefit from their clinical education and research experience and to provide safe patient care, including at times when they are not physically in the relevant clinical environment.

b) The University and the affiliated hospitals recognize that learners work at multiple sites and are expected to be able to access multiple systems.

[2] This is not intended to be an exhaustive list.

c) HICs have a responsibility to provide a data environment that is secure when properly used (a "secure institutional environment"), and to ensure mechanisms are available so learners can continue to provide patient care, if expected of them, outside of the clinical environment.

d) HICs have a responsibility to ensure that their institutional requirements are made available to learners.

e) Learners should not remove PHI from the secure (physical or virtual) central environment provided by the HIC unless there is no other reasonable means to provide safe and expedient patient care; and even when using PHI outside the secure central environment, learners must follow HIC policies for secure storage and use of PHI outside that environment.

f) Data used for teaching and/or learning purposes should be de-identified prior to transport out of the HIC's secure institutional environment, and confirmation should be obtained that the data will be accessed only by those needing to do so for those purposes, and that those accessing it will not attempt to re-identify individuals from the data. If identifiable information is necessary for the teaching and/or learning task, then it should be encrypted in accordance with HIC policy.

g) The HIC can disclose health information with the express consent of the patient or substitute decision-maker.

h) In certain circumstances, PHI must be disclosed (i.e. Child Protection, Ministry of Transportation, Health Protection and Promotion Act[3], Public Health).

i) PHI should be handled appropriately within the secure institutional environment. Learners must comply with all PHI and privacy policies and procedures of the HIC with custody of that PHI. When there is no alternative but to remove PHI from a secure institutional environment, the PHI must be fully de-identified, or otherwise fully protected. Hard copy data should not be left unattended; it should be kept hidden from unauthorized viewing, and kept in a locked case when not being used (for example, printed patient lists should be kept in a locked case or securely on the learner's person). Portable equipment used to transport PHI must be properly encrypted and password protected in accordance with HIC policy (for example, if a learner wished to store PHI on a USB key, the key must be encrypted using a HIC-approved method).

j) As professionals, learners must make fully informed decisions that take into account relevant risks and benefits. When faced with decisions regarding use of PHI to affect safe and efficient patient care, learners must consider both the relative risks posed by possible decisions on patient safety and possible breaches of confidentiality with respect to PHI. In the exceptional case where protecting privacy may significantly interfere with patient safety, patient safety must prevail. Specifically, if a HIC reasonably believes that a disclosure of PHI is needed to eliminate or reduce a significant risk of serious bodily harm, it is permitted to make that disclosure, without the consent of the individual to whom the PHI relates.[4]

[3] https://www.ontario.ca/laws/docs/90h07_e.doc
[4] PHIPA, section 40(1)

4. Access to and Authentication and Transmission of Personal Health Information:

Storage of PHI:

- The Information and Privacy Commissioner/Ontario has specifically advised all HICs that PHI must never be stored outside of secure institutional servers unless properly encrypted. PHI should be fully de-identified if held outside the secure institutional servers or networks if it is not encrypted. Electronic devices that are used to access, store, or record PHI, or by which PHI is transmitted must meet HIC-approved standards for information protection. In the current context, this includes: some type of authentication mechanism such as a power-on password, two-factor authentication, locking screen saver etc. to prevent access by unauthorized users, and the ability to encrypt stored and communicated PHI.

- If a learner chooses to use a personal handheld device to manage PHI, the learner must follow the applicable policies of the HIC to ensure that PHI will be sufficiently protected.

- Original hardcopy records must always remain in the secure institutional environment unless HIC policy permits otherwise.

Access to PHI:

- Learners must not access PHI on public access electronic devices or services.
- Using one's institutional login to access one's own personal health information or that of family and friends held within that institution, or networked data, is not typically permitted. Learners wishing to access information in their own personal patient record, must follow the same processes for acquiring access as any other patient would within the relevant institution.
- Access to network data should only be done by those within the direct circle of care.

Transmission of PHI:

- Learners may need to transmit PHI in connection with their clinical care responsibilities and educational needs. PHI must in these cases be protected in accordance with HIC policies. HICs, such as hospitals will provide access to secure methods and systems to support such transmission; provided that such transmission is in accordance with HIC policies. Learners must ensure that all systems and means they expose PHI to be appropriately secured, including, for example, recipient email servers, networks, and storage media. Specific examples in the current context, such as email accounts from Gmail, Hotmail, and Utoronto/UTmail+ are not considered secure for clinical information.

Removal of PHI:

- Learners may need to remove PHI from a secure institutional environment. PHI must in these cases be protected in accordance with HIC policies. Where necessary, HICs will provide HIC-approved equipment or applications, guidance and instructions to assist learners in encrypting data in accordance with their organizational policies.

- When learners take PHI outside of the secure institutional environment for approved purposes of teaching and learning (including at other HICs or in pure learning environments), all reasonable efforts to protect patient confidentiality must be undertaken. Specifically, participants should:
  - obtain the consent of the individuals to whom the PHI relates, if practical; or
  - adopt practices to de-identify PHI in accordance with HIC policy; and
  - ensure there are no patient identifiers associated with presentation materials; and
  - only disclose information that is general enough to preclude re-identification of the individuals ; and
  - ensure that anyone using the information is committed to using it only for the approved purposes and to refraining from attempting to re-identify any individual.

5. Reporting:

Learners must report any breach of information privacy or security, or the theft or loss of any device containing or permitting access to PHI immediately to both the educational authority to whom the learner reports and to the institutional HIC Privacy Officer.

6. Implications:

a. Breaches of PHI will be addressed under HIC policies and procedures, and consistent with PHIPA. Breach of any part of this statement may, after appropriate evaluation of the learner and the circumstances of the breach may result in further actions such as education, remediation, probation, dismissal from a course or program or failure to promote. In each case, a range of actions will be considered, and an action appropriate to the particular breach will be applied.[5]

b. This statement does not replace legal or ethical standards defined by organizations or bodies such as the College of Physicians and Surgeons of Ontario, the Canadian Medical Association, the Royal College of Physicians and Surgeons of Canada or the College of Family Physicians of Canada.

c. Action by an assessing body does not preclude action under other University or Institutional policy, or other civil remedies (under statute including PHIPA, the Criminal Code; or civil action).

[Original] Document Approved:
Undergraduate Medical Education Curriculum Committee – July 17, 2012
Physician Assistant Program Management Committee – July 16, 2012
Hospital University Education Committee – November 21, 2012
Postgraduate Medical Education Advisory Committee – November 23, 2012
Faculty Council Education Committee – Dec 6, 2012
Faculty Council – Feb 11, 2013
Hospital University Education Committee – May 17, 2017

[5] For MD Program students, the actions would be considered within the "Standards for grading and promotion of undergraduate medical students" For Postgraduate medical trainees, the actions would be considered within the "Guidelines for the Assessment of Postgraduate Residents of the Faculty of Medicine at the University of Toronto". For Fellows, the actions would be considered within the "Guidelines for Educational Responsibilities in Clinical Fellowships".