Temerty Medicine Social Media Task Force
Briefing Note

Proposed Revisions to the Temerty Medicine
Guidelines for Appropriate Use of the Internet, Electronic Networking and Other Media
and
Statement on Protection of Personal Health Information

March 22, 2023

Overview

In early 2022, a Social Media Working Group (since repositioned as a Task Force) was convened by the Dean's Executive to provide policy and operational recommendations that can help improve the social media user experience for Temerty Medicine community members. As part of its work, the Social Media Task Force (SMTF) reviewed relevant Temerty Medicine guidelines and statements to help ensure alignment with and appropriate reference to relevant University-level policies, guidelines and resources as well as reference to relevant external polices or guidelines (such as the CPSO Social Media Policy). The SMTF also considered possible gaps or areas for improvement/clarification in the relevant Temerty Medicine guidelines and statements.

The SMTF agreed that it would *not* be prudent to develop another Temerty Medicine guideline or statement specific to social media. Rather, the approach agreed upon by the SMTF was to incorporate more explicit language about social media into the following the following Temerty Medicine guidelines and statement:

- Guidelines for Appropriate Use of the Internet, Electronic Networking and Other Media
- Statement on Protection of Personal Health Information

The SMTF endorsed revisions to those two documents, as summarized below. A proposed revision common to these two documents is expansion of scope such that they apply to all Temerty Medicine learners, including those registered or participating in educational activities affiliated with the Temerty Medicine, who may during their studies, training and/or research activities have contact with patients and/or patient information. It is important to note that learner interactions with patients and patient information is particular focus of the guidelines and statement under consideration, which distinguishes these two documents from relevant University-level policies, guidelines and resources.

Copies of the revised guidelines and statement are included as appendices.

Proposed Revisions

- Guidelines for Appropriate Use of the Internet, Electronic Networking and Other Media

  These guidelines, which were last updated in 2020 to more explicitly reference social media, currently apply to all medical learners registered at Temerty Medicine, including undergraduate and postgraduate students, fellows, clinical research fellows, or equivalent. The SMTF proposes:
  - expansion of the scope of the guidelines such that they apply to all Temerty Medicine learners, including those registered or participating in educational activities affiliated with the Temerty Medicine, who may during their studies, training and/or research activities have contact with patients and/or patient information
  - additional language in the preamble, essentially taken verbatim from the 2022 "Social Media Resources and Supports for Faculty Members and Librarians" document that was developed centrally, to indicate that no member of the University should engage in hate speech or in behaviour that demeans, harasses,

or intimidates others, and that no member of the Temerty Medicine community should be subject to such language or behaviours in the course of their University work or study
  - editorial revisions to more explicitly reference relevant University of Toronto policies (i.e. Code of Student Conduct, Policy on Sexual Violence and Sexual Harassment, Statement on Prohibited Discrimination and Discriminatory Harassment, and Standards of Professional Practice Behaviour for all Health Professional Students), the CPSO Social Media Policy, and the Temerty Medicine Statement on Protection of Personal Health Information
  - revisions to the "Enforcement" section of the policy to clarify that concerns regarding inappropriate use will be addressed on a case-by-case basis in accordance with the relevant guidelines and procedures

- Statement on Protection of Personal Health Information

  This statement currently 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. The working group endorsed:
  - expansion of the scope of the statement such that it applies to all Temerty Medicine learners, including those registered or participating in educational activities affiliated with Temerty Medicine, who may during their studies, training and/or research activities have contact with patients and/or patient information
  - editorial revisions that more explicitly reference social media

Consultations and Approvals

With respect to consultation, the proposed revisions were informed feedback from SMTF members, which includes representatives from various decanal-level portfolios; faculty representatives from the basic science, clinical and rehabilitation science departments; learners from across Temerty Medicine education programs; and administrative staff from across Temerty Medicine.

The proposed revisions have also been informed by feedback provided by various Temerty Medicine education leaders, including the Vice Dean, Research and Health Science Education; Associate Dean, Undergraduate Education; Director, Rehabilitation Sciences Institute; and Chair, Department of Physical Therapy. Consultation emails have been sent to the Director, Institute of Medical Science, Temerty Medicine; Acting Vice-Dean, Research and Program Innovation, School of Graduate Studies; and Acting Vice-Dean, Undergraduate, Arts & Science.

The proposed revisions were approved by the Hospital-University Education Committee (HUEC) at its March 22, 2023 meeting.

Given proposed expansion of scope, the SMTF assumes that Temerty Medicine Faculty Council would be the ultimate approval body, pending review by the relevant committees of Faculty Council.

Guidelines for
Appropriate Use of the Internet, Electronic Networking and Other Media

Date of original approval: 2008
Date of last revision and approval: PGMEAC April 2008; HUEC June 2008; HUEC 2020

Scope
This statement applies to all Temerty Medicine learners, including those registered or participating in educational activities affiliated with the Temerty Medicine, who may in the course of their studies, training and/or research activities have contact with patients and/or patient information.

Internet, electronic networking and other media includes emails sent or received, email accounts, digital music, digital photographs, digital means and videos, social networks, file sharing accounts, other online accounts and similar digital items which currently exist or may exist as technology develops, regardless of the ownership of a physical device or digital item that is stored.

The use of the Internet, electronic networking and other media includes but is not limited to posting/commenting on blogs; direct messaging (DM), instant messaging (IM), private messaging (PM) on social networking sites; posting to public media sites, mailing lists and video-sites; and emails.

These Guidelines are informed by but do not replace or limit the standards established by professional or regulatory bodies; by relevant clinical settings; or by other applicable University or Faculty standards, policies, and procedures, including those referenced throughout this document and listed in Appendix A.

Preamble
The capacity to record, store and transmit information in electronic format brings specific responsibilities to those working in healthcare with respect to privacy of patient information and ensuring public trust in our hospitals, institutions and practices. Significant educational benefits can be derived from this technology and learners need to be aware that there are also potential problems and liabilities associated with its use. Material that identifies patients, institutions or colleagues and is intentionally or unintentionally placed in the public domain may constitute a breach of standards of professionalism and confidentiality that damages the profession and our institutions. Guidance for Temerty Medicine learners about appropriate use of the Internet, electronic networking and other media is necessary to avoid problems while maintaining the University of Toronto's commitment to freedom of expression.

Various statements, policies, protocols, codes and standards apply to social media communications (see Appendix A). In particular, no member of the University should engage in hate speech or in behaviour that demeans, harasses, or intimidates others; nor should any community member be subject to such language or behaviours in the course of their University work or study. The University is committed to providing support to members of our community who are experiencing harassment or intimidation in social media spaces and to exploring intervention options via its policies and procedures or through municipal law enforcement where circumstances permit.

Postgraduate medical learners are reminded that they must meet multiple obligations in their capacity as university students, as members of their profession and relevant professional regulatory bodies, and as employees of hospitals and other institutions. Undergraduate and professional master's learners are reminded that they must meet multiple obligations in their capacity as university students and as future members of

their professions. For all Temerty Medicine learners, these obligations extend to the use of the Internet, electronic networking and other media at any time – whether in a private or public forum.

General Guidelines for Safe Use of the Internet, Electronic Networking and Other Media

These Guidelines are based on several foundational principles, as follows:

- The importance of privacy and confidentiality to the development of trust between health care practitioner and patient.
- Respect for colleagues and co-workers in an inter-professional environment.
- The tone and content of electronic conversations should remain professional.
- Individuals are personally responsible for the content published on or disseminated using the Internet, electronic networking or other media.
- The assumption that material published on or disseminated using the internet, electronic networking or other media is permanent.
- All involved in health care have an obligation to maintain the privacy and security of patient records under the Personal Health Information Protection Act (PHIPA), which defines a record as "information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise".

a) Professional Behaviour

All Temerty Medicine learners will engage in behaviour that displays and reflects truth, honesty, representation in, on and around electronic platforms and/or devices. Learners are to engage only in on-line activities that are respectful and exemplify professional behaviour that would preclude cyberbullying.

Inappropriate use of the Internet, electronic networking or other media may breach University of Toronto codes of behaviour, including the Code of Student Conduct, Policy on Sexual Violence and Sexual Harassment, Statement on Prohibited Discrimination and Discriminatory Harassment, and Standards of Professional Practice Behaviour for all Health Professional Students. Inappropriate use of the Internet, electronic networking or other media may also breach standards established by professional or regulatory bodies, including for medical learners the CPSO Social Media Policy.

b) Posting Information about Patients

Never post personal health information about an individual patient.

Personal health information (PHI) is defined in the Personal Health Information Protection Act (PHIPA) as any information about an individual in oral or recorded form, where the information "identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual".

These guidelines apply even if the individual patient is the only person who may be able to identify theirself on the basis of the posted description. Learners should ensure that anonymised descriptions do not contain information that will enable *any* person, including people who have access to other sources of information about a patient, to identify the individuals described.

Further guidance is provided in the Temerty Medicine Statement on Protection of Personal Health Information, which sets out requirements to ensure appropriate access to and use of Personal Health Information in affiliated teaching sites' custody by Temerty Medicine learners.

Exceptions *that would be considered appropriate use of the Internet, electronic networking and other media*.

It is appropriate to post information about patients:

1. With the express consent of the patient or substitute decision-maker.
2. Within secure internal hospital networks if expressly approved by the hospital or institution. Please refer to the specific internal policies of your hospital or institution.
3. Within specific secure course-based environments provided by the University of Toronto that are password-protected or have otherwise been made secure. Even within these course-based environments, participants should:
    a. adopt practices to "anonymise" individuals;
    b. ensure there are no patient identifiers associated with presentation materials; and
    c. use objective rather than subjective language to describe patient behaviour. For these purposes, all events involving an individual patient should be described as objectively as possible, i.e., describe a hostile person by simply stating the facts, such as what the person said or did and surrounding circumstances or response of staff, without using derogatory or judgmental language.
4. When using entirely fictionalized accounts that are so labelled.

c) Professional Communication With and Posting Information About Colleagues and Co-Workers

Respect for colleagues and co-workers, including their privacy rights, is important in an interprofessional working environment. Addressing colleagues and co-workers in a manner that is insulting, abusive or demeaning is unprofessional behaviour. Making demeaning or insulting comments about colleagues and co-workers to third parties, including via the Internet, electronic networking and other media, is also unprofessional behaviour. If you are in doubt about whether it is appropriate to post any information about colleagues and co-workers, ask for their explicit permission – preferably in writing.

Insulting, abusive or demeaning comments and communication may breach University of Toronto codes of behaviour and/or standards established by professional or regulatory bodies, including those referenced in (a) above.

d) Posting Information Concerning Hospitals or other Institutions

Learners should comply with hospital or institutional policies regarding the use of technology as well as the use of any proprietary information such as logos or mastheads.

Learners must not represent or imply that they are expressing the opinion of the organization. Be aware of the need for a hospital as well as the University of Toronto to maintain the public trust. Consult with the appropriate resources such as the relevant communications or public relations office at the hospital or Temerty Medicine.

e) Offering Clinical Advice

Do not misrepresent or mislead as to your qualifications or role.

The provision of medical advice by postgraduate medical learners is governed by the terms of their registration with the College of Physicians and Surgeons of Ontario, which limits the provision of medical advice by postgraduate medical learners within the context of the teaching environment. Provision of medical advice by postgraduate medical learners outside of this context is inconsistent with the terms of educational registration.

Similarly, the provision of clinical advice by other professional clinical learners is governed by the terms of their registration with their professional regulatory bodies.

f) Academic Integrity Extends to the Appropriate Use of the Internet, Electronic Networking and Other Media

The University of Toronto's Code of Behaviour on Academic Matters articulates offences that are considered a breach of academic integrity. These offences include plagiarism and forms of cheating such as sharing examination questions or collaborating on work where specifically instructed not to do so.

Enforcement (Disclosure and Reporting)

All professionals have a collective professional duty to assure appropriate behaviour, particularly in matters of privacy and confidentiality.

If an individual observes or experiences a Temerty Medicine learner potentially breaching these Guidelines, and if the individual feels comfortable, willing, and judges that it is safe to do so, they may choose to approach the learner and communicate their concerns with the goal of ending the behaviour. This approach recognizes the important role of collegial conversation in the medical community, and emphasizes the principle of addressing problems locally and on a case-by-case basis wherever possible.

However, if such a conversation is inappropriate in the circumstances (e.g., it has previously been ineffective, or if more support is required due to a significant power imbalance) then an individual who observes or experiences concerning behaviour may disclose their concerns to a member of the University community with whom they feel comfortable (e.g., their course or program director, Office of Learner Affairs, Learner Experience Unit). It will be the choice of the individual who witnessed or experienced the concerning behaviour to make a disclosure or formal report, ideally following discussion with a knowledgeable and trusted education leader or office about the appropriate reporting pathways and procedures. Such concerns will be addressed on a case-by-case basis, in accordance with the relevant guidelines and procedures.

Complaints about breaches of privacy may be filed with the Information and Privacy Commissioner of Ontario.

Penalties for Inappropriate Use of the Internet, Electronic Networking and Other Media

Penalties for inappropriate use of the Internet, electronic networking and other media include:

- Remediation, failure to promote, probation or dismissal by the Temerty Faculty of Medicine
- A finding of professional misconduct by the College of Physicians and Surgeons of Ontario or other professional regulatory body
- Prosecution or a lawsuit for damages for a contravention of the PHIPA

Appendix A – Associated Statements, Policies, Protocols, Codes and Standards

University of Toronto

- Appropriate Use of Information and Communication Technology
- Code of Student Conduct
- Standards of Professional Practice Behaviour for all Health Professional Students
- Statement on Prohibited Discrimination and Discriminatory Harassment
- Policy on Sexual Violence and Sexual Harassment
- Protocol with Health Care Institutions: Sexual Violence and Sexual Harassment Complaints involving Faculty Members and Students of the University of Toronto arising in Independent Research Institutions, Health Care Institutions and Teaching Agencies
- Code of Behaviour on Academic Matters

Temerty Faculty of Medicine

- Temerty Medicine Statement on Protection of Personal Health Information
- MD Program Student Mistreatment Protocol
- PGME Guideline for Managing Disclosures about Learner Mistreatment

College of Physician and Surgeons of Ontario

- Social Media policy and Advice to the Profession companion document
- Professional Responsibilities in Medical Education policy
- Protecting Personal Health Information policy
- Physician Behavior in the Professional Environment policy and Guidebook for Managing Disruptive Physician Behaviour

Government of Ontario

- Ontario Human Rights Code
- Personal Health Information Protection Act
- Information and Privacy Commissioner of Ontario

Hospitals and research institutes affiliated with the University of Toronto

- Contact the relevant hospital/research centre

Statement on Protection of Personal Health Information

Date of original approval by Faculty Council: February 11, 2013 **Date of last review by the Hospital University Education Committee (HUEC)**: May 17, 2017

1. Scope

This statement was developed to provide guidance for the protection of Personal Health Information (PHI) by Temerty Medicine learners in the context of Health Information Custodians (HICs) as integral components of the learning environment. This statement applies to all Temerty Medicine learners, including those registered or participating in educational activities affiliated with the Temerty Medicine, who may in the course of their studies, training and/or research activities have contact with patients and/or patient information.

2. Background and Rationale

Personal health information is defined in the Personal Health Information Protection Act (PHIPA) as any information about an individual, in oral or recorded form, where the information "identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual". This includes identifiable information such as name, address, identifying numbers and other unique characteristics.

This statement sets out requirements to ensure that all recorded (hardcopy and digital) forms of Personal Health Information (PHI) 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 reidentified, if context and other information known outside of the circle of care could still be used to reidentify 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 the PHIPA, which 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 disposal. Learners engage in patient care and education/research involving access to PHI through the affiliation agreements between the University of Toronto and the Hospitals and in other healthcare placements. As agents of HICs, learners are permitted to use PHI. Accordingly, learners must be aware of and comply with the HICs' requirements and the HICs must make those requirements known to learners.

Learners need access to systems containing PHI 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

and/or research. Once PHI is no longer required by the learner to provide patient care within a given institution or proceed with their research experience, 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, digital, and any form of information technology) that could be used to store or transmit PHI. This includes but is not limited to posting/commenting on blogs; direct messaging (DM), instant messaging (IM), private messaging (PM) on social networking sites; posting to public media sites, mailing lists and video-sites; and emails. Further guidance regarding appropriate use of the Internet, electronic networking and other media by Temerty Medicine leaners is provided in the Temerty Medicine Guidelines for Appropriate Use of the Internet, Electronic Networking and Other Media.

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.

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 disseminated 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 decisionmaker.

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

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 (see PHIPA, section 40).

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

Storage of PHI:

- The Information and Privacy Commissioner of 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.
- 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.

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:
Breaches of PHI will be addressed under HIC policies and procedures, consistent with the 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, failure to promote, dismissal from a course or program. In each case, consideration of the matter by Temerty Medicine, including the range of academic sanctions, will be informed by the relevant guidelines and procedures.

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, the College of Family Physicians of Canada, or the College of Physiotherapists of Ontario.

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).

Review and Approval History
Original document:
- 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

Review:

- Hospital University Education Committee – May 17, 2017