NOSM UNIVERSITY | Continuing Education and Professional Development

POLICY

NOSM University CEPD Office Privacy Policy
Approved By: CEPD Governance Committee
Established on: September 18, 2008
Revision Date: September 19, 2024

1.0 POLICY STATEMENT

The CEPD Privacy Policy exists to provide guidance for staff, faculty, and scientific planning committee (SPC) members, on NOSM U CEPD Office processes for ensuring the privacy of all personal information collected in relation to the development and delivery of accredited activities.

2.0 SCOPE

This Privacy Policy is intended to assist NOSM U staff, faculty, preceptors, and learners to understand their obligations under the Freedom of Information and Protection of Privacy Act (FIPPA) as they relate to the development and delivery of accredited CPD activities. It is not intended to be a substitute for legal advice. If you have specific questions about FIPPA, please contact the NOSM University Human Resources Unit.

This policy applies to:

- Planning committee members
- Participants in CPD activities
- Speakers, facilitators, moderators and authors involved with the CPD activity
- Patients, family members or learners being discussed in case studies presented at CPD activities

Exclusions from this policy per the Information and Privacy Commissioner of Ontario:

FIPPA specifically excludes from the definition of personal information, the name, title, contact information or designation that identifies a person in a business, professional or official capacity. This includes a business carried out in a home.

As a general rule, information about an individual in a business, professional or official capacity is not considered to be personal information.

****Note:** If information relates to an individual in a business capacity, it may still qualify as personal information if it reveals something of a personal nature about the individual. The context in which the information appears is important.

Kind of Information that may be collected:

- Your Internet Protocol (IP) address and browser-type

- The date and time of your visit to a CEPD website or participation in an educational activity
- The pages visited within NOSM U CEPD sites (May include, but not limited to: Fourwaves, SharePoint, WordPress, Qualtrics, WebEx, Teams, Colleague)
- Planning committee member name, community, College affiliation
- Speaker name, address, payment details
- Presentations/Case presentations may include details of a clinical case or educational scenario, however unique identifiers must be removed

3.0 DEFINITIONS

Accreditation:
The CFPC and RCPSC use different terminology to describe successfully meeting the administrative, educational and ethical standards set by each College in the development of Continuing Professional Development (CPD) and Faculty Development (FD) educational activities. The universal terminology, and the terminology used by the RCPSC is ***accreditation***, while the CFPC refers to the same process as ***certification***.

Continuing Professional Development (CPD) Activity:
An educational activity that has a clinical or faculty development focus, and is based on identified learning needs, has learning objectives, and is evaluated to assure the learning objectives are met. A CPD/educational activity is distinct from a social event. **Note that CPD and educational activity may be used interchangeably.

CPD Provider Organization (CFPC Term):
An organization that assumes responsibility and accountability for the development, delivery, and evaluation of Mainpro+ certified CPD activities. The CPD provider organization must form a scientific planning committee—independent of sponsor influence—to conduct this work.

Educational) Activity:
An educational offering that is part of the Continuing Professional Development (CPD) provider organization's overall programming or one for which the CPD provider organization grants credit(s). **Note that CPD and educational activity may be used interchangeably.

Identifiable Individual:
Information is about an identifiable individual if:

a) it is about the individual in a personal capacity; that is, it reveals something of a personal nature about the individual, and
b) it is reasonable to expect that an individual can be identified from the information (either alone or by combining it with other information)

Examples include a person's name when combined with other information about them, such as their address, sex, age, education, or medical history. These examples are not exhaustive, and many other kinds of information may still qualify as personal information.

Healthcare/Pharmaceutical Industry (HPI):
Commercial entities that develop, produce, market, resell, or distribute drugs, devices, products, or other healthcare goods, services, or therapies that may be prescribed to patients or ordered by physicians or other regulated health professional, in the diagnosis, treatment, monitoring,

management, or palliation of health conditions. Examples include (but are not limited to): Pharmaceutical companies, medical device companies, medical and surgical supply companies, producers of non-prescription healthcare products, nutrition companies (infant formula, nutritional supplements), pharmacies; diet, fitness, and weight-loss companies; prosthetic and orthotic stores; hearing test centres; home care companies; etc., or clinical services that are owned or controlled by any of the above entities. *(From CFPC Understanding Mainpro+ Certification 2021)*

Participant:
A person enrolled In a CPD activity, whose learning needs have priority. Participants are responsible for identifying their own gaps in knowledge, skill or attitude, actively participating in filling them, and keeping track of their learning gains.

Personal Information:
Recorded information about an identifiable individual, including:

a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual
b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved
c) any identifying number, symbol or other particular assigned to the individual
d) the address, telephone number, fingerprints or blood type of the individual
e) the personal opinions or views of the individual except where they relate to another individual
f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence
g) the views or opinions of another individual about the individual
h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.
i) Information about an individual is not personal information, only if they have been dead for more than thirty years.

Privacy:
The rules regarding the collection, retention, use, disclosure and disposal of personal information in its custody or control.

Privacy Breach:

A privacy breach is the improper or unauthorized access to, creation, collection, use, disclosure, retention or disposal of personal information.

Privacy breaches may occur because of innocent mistakes or intentional actions by:

- NOSM U or CEPD employees
- SPC members or administrative staff
- Host organizations of SPCs
- Sponsoring organizations

- outside parties who have malicious intent
- other internal or external parties

Recorded Information:
Information recorded in any format, such as paper records, electronic records, digital photographs, videos or maps.

Sponsor:
A company, organization, institution, government agency or other entity (for-profit or not-for-profit) that contributes financial or in-kind resources to a CPD course or other activity.

4.0 POLICY TERMS OR PROCEDURES

4.1 Relevant FIPPA Sections:

38(2) Collection of personal information

No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity. R.S.O. 1990, c. F.31, s. 38 (2).

Retention of personal information

40 (1) Personal information that has been used by an institution shall be retained after use by the institution for the period prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the personal information. R.S.O. 1990, c. F.31, s. 40 (1).

Manner of collection

39 (1) Personal information shall only be collected by an institution directly from the individual to whom the information relates unless,

(a) the individual authorizes another manner of collection

Notice to individual

(2) Where personal information is collected on behalf of an institution, the head shall, unless notice is waived by the responsible minister, inform the individual to whom the information relates of:

a) the legal authority for the collection;
b) the principal purpose or purposes for which the personal information is intended to be used; and
c) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection. R.S.O. 1990, c. F.31, s. 39 (2).

Use of personal information

41(1) An institution shall not use personal information in its custody or under its control except:

a) (a) where the person to whom the information relates has identified that information in particular and consented to its use;
b) (b) for the purpose for which it was obtained or compiled or for a consistent purpose;
c) (c) for a purpose for which the information may be disclosed to the institution under section 42 or under section 32 of the *Municipal Freedom of Information and Protection of Privacy Act*; or
d) (d) subject to subsection (2), an educational institution may use personal information in its alumni records and a hospital may use personal information in its records for the purpose of its own fundraising activities, if the personal information is reasonably necessary for the fundraising activities. R.S.O. 1990, c. F.31, s. 41; 2005, c. 28, Sched. F, s. 5 (1); 2010, c. 25, s. 24 (9).

Notice on using personal information for fundraising

41(2) In order for an educational institution to use personal information in its alumni records or for a hospital to use personal information in its records, either for its own fundraising activities or for the fundraising activities of an associated foundation, the educational institution or hospital shall:

a) give notice to the individual to whom the personal information relates when the individual is first contacted for the purpose of soliciting funds for fundraising of his or her right to request that the information cease to be used for fundraising purposes;
b) periodically and in the course of soliciting funds for fundraising, give notice to the individual to whom the personal information relates of his or her right to request that the information cease to be used for fundraising purposes; and
c) periodically and in a manner that is likely to come to the attention of individuals who may be solicited for fundraising, publish a notice of the individual's right to request that the individual's personal information cease to be used for fundraising purposes. 2005, c. 28, Sched. F, s. 5 (2); 2010, c. 25, s. 24 (10).

Where disclosure permitted

42 (1) An institution shall not disclose personal information in its custody or under its control except:

a) where the person to whom the information relates has identified that information in particular and consented to its disclosure
b) for the purpose for which it was obtained or compiled or for a consistent purpose
c) where disclosure is made to an officer, employee, consultant or agent of the institution who needs the record in the performance of their duties and where disclosure is necessary and proper in the discharge of the institution's functions
d) in compassionate circumstances, to facilitate contact with the spouse, a close relative or a friend of an individual who is injured, ill or deceased
e) subject to subsection (2), an educational institution may disclose personal information in its alumni records, and a hospital may disclose personal information in its records, for the purpose of its own fundraising activities or the fundraising activities of an associated foundation if:
    1) the educational institution and the person to whom the information is disclosed, or the hospital and the person to whom the information is

disclosed, have entered into a written agreement that satisfies the requirements of subsection (3), and

2) the personal information is reasonably necessary for the fundraising activities. R.S.O. 1990, c. F.31, s. 42; 2005, c. 28, Sched. F, s. 6 (1); 2006, c. 19, Sched. N, s. 1 (5-7); 2006, c. 34, Sched. C, s. 5; 2010, c. 25, s. 24 (12); 2019, c. 7, Sched. 31, s. 4.

Meaning of de-identification

49.1(2) A reference in this Part to de-identifying a record or personal information means to remove the following information:

1. Information that identifies an individual.

2. Information that could be used, either alone or with other information, to identify an individual based on what is reasonably foreseeable in the circumstances. 2019, c. 7, Sched. 31, s. 6.

Purpose for the collection of personal information

49.2 The purpose of the collection of personal information under this Part is to compile information, including statistical information, to enable analysis in relation to,

(a) the management or allocation of resources.

(b) the planning for the delivery of programs and services; and

(c) the evaluation of those programs and services. 2019, c. 7, Sched. 31, s. 6.

4.2 Planning committee members

4.2.1 Personal Information collected from planning committee members for the purposes of completing the conflict-of-interest disclosure or other declaration will be retained by the planning committee in a secure file, for a period of 7 years.

4.2.2 Personal information of planning committee members provided to the CEPD Office as part of the accreditation application, will be reviewed only by the coordinator, accreditation coordinator and the medical reviewers involved in the review of each application respectively.

4.2.3 Where a concern is identified in the application and escalation of the review is necessary, confidential information may also be shared with the CEPD CME Medical Director and the CEPD Associate Dean.

4.2.4 All personal records related to planning committee members is stored in the secure SharePoint CEPD document library for a period of seven years.

4.3 Participants in CPD activities

4.3.1 Participant information collected through the registration process is retained by the SPC for a period of seven years, in compliance with record retention requirements of the CFPC and RCPSC standards.

4.3.2 Participant information may be collected through the evaluation process, where programs have incorporated the option for participants to extract their certificate of participation via a sub-survey of the evaluation process.

4.3.3 During face-to-face educational activities, registration and attendance lists are kept confidentially by the SPC designate on site.

4.3.3.1 Registration lists and attendance lists are not shared with sponsoring or other organizations at the activity.

4.3.3.2 Registration lists and attendance records are not shared with sponsoring organizations in any post event communications.

4.3.3.3 Sponsoring organizations on site will be placed in a designated area, and participants have the option of visiting the exhibit hall and sharing any personal information related to draws or the mailing of product/company information, at their own discretion.

4.3.4 During virtual activities, participants are informed during the registration process, that:

4.3.4.1 Sponsors may be on the call and will see the names of participants unless the log into the activity with an abbreviated or nickname.

4.3.4.2 Participants are given the option to log into virtual sponsor ‘rooms’ and participate in or share any personal information at their own discretion.

4.3.5 In the event that a sponsoring organization requests information regarding the participants registered in the activity, no personal information is to be shared. Instead SPC’s are encouraged to share data related to the types of participants and perhaps communities reached.

4.4 Speakers, facilitators, moderators and authors involved with the CPD activity

4.4.1 Personal Information collected from speakers for the purposes of completing the conflict-of-interest disclosure or other declaration will be retained by the planning committee in a secure file, for a period of 7 years.

4.4.2 Personal information of speakers provided to the CEPD Office as part of the accreditation application, will be reviewed only by the coordinator, accreditation coordinator and the medical reviewers involved in the review of each application respectively.

4.4.3 Where a concern is identified in the application and escalation of the review is necessary, confidential information may also be shared with the CEPD CME Medical Director and the CEPD Associate Dean.

4.4.4 Personal information collected from speakers for the purposes of payment, is to be stored in alignment with PCI Compliance in Canada (a set of comprehensive requirements all businesses that handle credit and debit payments must comply with, regardless of size or number of transactions they process).

4.4.4.1 Payments processed through the CEPD Office and NOSM U Finance Office will be done so through the perceptive software operated by the NOSM U Finance Unit.

4.4.5 Speakers complete a release that provides them the opportunity to opt out of being broadcast virtually, recorded, or having their presentation archived and available for later viewing. Included in the release is a place for the speaker to confirm that any reference to patient cases discussed will have all unique identifiers that when combined would lead to the identification of an individual removed, (including but not limited to: name, age, date of birth, or image of

the patient), so that the patient cannot reasonably be identified, or that they have obtained written approval from the patient to share their information.

4.4.6 All personal records related to speakers are stored in the secure SharePoint CEPD document library for a period of seven years.

4.5 Patients, family members or learners being discussed in case studies presented at CPD activities

4.5.1 It is the responsibility of the SPC to ensure that the speaker release is completed prior to the educational activity.

4.5.2 It is the responsibility of the SPC to review presentations and ensure that any unique identifiers have been removed from the presentation.

4.6 Privacy Breach

4.6.1 A privacy breach occurs when personal information is accessed, collected, used, disclosed or disposed of without proper authorization.

4.6.2 Inappropriate use or disclosure of this information may constitute a breach of the Freedom of Information and Protection of Privacy Act (FIPPA) and may have a significant, even devastating, impact upon the affected individuals as well as reputational and financial harm to the CEPD Office and NOSM University.

4.6.3 Re the CEPD Office: As a general rule, NOSM U CEPD faculty and staff members are authorized to access personal information on a “need to-know” basis, whereas individuals who are not faculty or staff are only authorized to access personal information under exceptional circumstances and with permission of the CEPD Director. If you are not sure whether access was authorized, you should check with the CEPD Director.

4.6.4 Re Community-based SPC’s and Physician Organizations: If a privacy breach has occurred, contact the Chair of the SPC, and/or the Physician Organization.

4.6.5 Privacy Breach Management Steps:

1. Report the breach to the CEPD Director or SPC Chair
2. Determine the cause of the breach:
    - the theft, loss or disappearance of equipment or devices that contain personal information that were not sufficiently encrypted
    - lost documents in an office
    - an email that contains personal information sent to an unintended recipient
    - unintended disclosure of the identities of other recipients of a sensitive email sent in carbon copy (cc) instead of blind carbon copy (bcc), for example, an email pertaining to a personnel selection process
    - phishing or the use of deceptive tactics to trick an employee into providing their personal information either directly or by going to a fake website
    - collecting personal information that isn’t directly related or necessary for a program
    - accessing of participant data through unapproved access to registration or attendance lists
    - using personal information for a purpose that isn’t consistent with the purpose for which it was originally collected

- unauthorized access to personal information, such as snooping
- a cyber attack affecting one of the CEPD platforms or platforms managed by the SPC.

3. Involve the appropriate authority to manage containment of the breach

5.0 ROLES AND RESPONSIBILITIES

5.1 CEPD Office: It is the responsibility of the CEPD Office to ensure that SPC's have the necessary resources and guiding documents to ensure that program development adheres to the FIPPA Act and with CACME privacy standards.

5.2 Scientific Planning Committee/Physician Organization: The SPC or physician organization must ensure adherence to the FIPPA Act as presented in this document.

5.3 Sponsor: The sponsoring organization must abide by Innovative Medicines Canada Code of Ethical Practices and respect the FIPPA privacy standards for each educational activity.

6.0 INTERPRETATION

It is important to examine the context in which information appears, in determining whether the information is "about" an individual and whether the individual is "identifiable." Depending on the context, information may not meet the definition of personal information because it is, for example, information about a property or business, or about an individual in a business capacity.

7.0 RELATED DOCUMENTS

7.1 Speaker Release Form

AUTHORITIES AND OFFICERS

The following is a list of authorities and officers for this policy:

a. Approving Authority: CEPD Governance Committee

b. Procedural Authority: CEPD Director

Review and Revision History

Review Period: Every 2 years or as required

Date for Next Review: September 2026