Fleming College

Procedure Title:	Use and Disclosure of Personal Health Information Procedure (PHIPA)
Procedure ID:	#OP 1-112D
Manual Classification:	Section 1 – College Policies
Linked to Policy:	#1-112 Information Practices Related to Personal Health Information
Approved by Senior Management Team:	February 24, 2021
Revision Date(s):	N/A
Effective Date:	March 1, 2021
Next Policy Review Date:	March 2023
Contacts for Policy Interpretation:	Policy and Privacy Officer

1.0 – Purpose

The purpose of this procedure (the "**Procedure**") is to set out instructions for members of the College Community on how to use and disclose Personal Health Information in accordance with the College's Information Practices related to Personal Health Information and the *Personal Health Information Protection Act* ("**PHIPA**").

The College is a Health Information Custodian as it provides the following 3 health services: (1) Counselling Services (2) Health Services and, (3) the Massage Clinic (each a "**College Health Service**" and collectively the "**College Health Services**"). For the purpose of this Procedure, the "individual" is to mean the patient of one or more of the College Health Services. Capital terms not defined in this Procedure have the same meaning found in the College's Information Practices related to Personal Health Information.

2.0 – Use of Personal Health Information

The term "**use**" is defined under PHIPA. It means to access, view, handle or otherwise deal with Personal Health Information, but does not include disclosure. The College may provide the Personal Health Information to its Agents to use it for the same reasons for which the PHI was collected. The sharing of Personal Health Information between the College and its Agent is considered a use and not a disclosure or collection for the purposes of PHIPA.

When using Personal Health Information the College:

- Must have consent to use an individual's Personal Health Information, for the purpose(s) specified in the consent, or as permitted by law and only to the extent as is reasonably necessary or required by law, unless PHIPA allows the PHI to be used without consent (see the list below for examples of use without consent);

- May not use Personal Health Information if other information would serve the purpose specified in the consent;

- May only use as much Personal Health Information as necessary to meet the purpose specified in the consent; and

- Must take reasonable steps to ensure that the individual's Personal Health Information is as accurate, complete and up-to-date as necessary for the purpose specified in the consent.

The College may use Personal Health Information about an individual without consent:

- For the purposes for which it was collected or created and for all the functions reasonably necessary for carrying out that purpose, subject to exceptions;

- To plan or deliver its programs or services;

- For risk management, error management or activities to improve or maintain the quality of care or any related program or service;

- To educate its Agents (such as nursing students) to provide health care;

- To obtain payment or to process, monitor, verify or reimburse health care claims;

- For research, provided that specific requirements regarding the preparation of a research plan and approval by a research ethics board, as outlined in PHIPA, are met;

- For the purposes for which another person was permitted or required by law to disclose the PHI to the College; and

- If permitted or required by law.

If the College is permitted to use Personal Health Information without consent for any purpose, the College may provide that PHI to its Agent for that purpose.

3.0 – Disclosure of Personal Health Information

The term "**disclose**" means to make the Personal Health Information available or to release it to another Health Information Custodian or person. Disclosing does not include providing Personal Health Information back to the person who provided or disclosed it in the first place, whether or not the Personal Health Information has been manipulated or altered, as long as it does not include additional identifying information.

The disclosure of Personal Health Information by the College must comply with the following:

- The College must have consent to disclose an individual's Personal Health Information, for the purpose(s) specified in the consent, or as permitted by law and only to the extent

as is reasonably necessary or required by law, unless PHIPA allows it to be disclosed without consent (see below list of examples of disclosure without consent);

- If relying on implied consent, the College must ensure the requirements are fulfilled for the disclosure of Personal Health Information within the "**Circle of Care**" only for the purpose of health care and the individual has not expressly withheld or withdraw consent;

- Unless permitted or required by law, express consent is generally required when the Personal Health Information is disclosed by the College to a non-Health Information Custodian, where the College discloses to another Health information Custodian for a purpose other than health care or for market research, and fundraising, if more than contact information is provided;

- The College must take reasonable steps to ensure no Personal Health information is disclosed inadvertently to unintended recipients; and

- The College must also take reasonable steps to ensure that the Personal Health Information is as accurate, complete and current as is necessary for the purpose(s) of disclosure or clearly sets out the limitations if any.

The College may disclose Personal Health Information to another person or organization in the following circumstances without the individual's consent, but only as permitted or required by law. The following are examples of such disclosures without consent:

- To provide health care, and consent cannot be obtained in a timely manner, unless there is an express request from the individual instructing otherwise;

- To provide funding to the College Health Services by the Ministry of Health for the provision of health care;

- To eliminate or reduce a significant risk of serious bodily harm to a person or group of persons (for example, disclosure to a student's family or physician if the psychologist believes that it is necessary to reduce the risk of the student's suicide);

- To contact a relative, friend or substitute decision-maker if the individual is injured, incapacitated or ill and unable to give consent;

- To transfer Records to the archives for conservation;

- To carry out an inspection, investigation or similar procedure that is authorized by a warrant, PHIPA or another Act;

- To determine or verify eligibility for publicly funded health care or related goods, services or benefits;

- To administer or enforce various acts by the professional colleges and other regulatory bodies;

- To a prescribed person that complies and maintains a registry of Personal Health Information for the purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily substance;

- To a prescribed entity for the purpose of analysis or compiling information with respect to management, evaluation or monitoring of the health system;

- To the Public Guardian and Trustee, a children's aid society and the Children's Lawyer for the purpose of carrying out their statutory functions

- To a person conducting an audit or reviewing an accreditation or application for accreditation related to the services of a custodian;

- To identify an individual who is deceased or is reasonably suspected to be deceased or for informing people when it is reasonable inform, that the individual is deceased or reasonably suspected to be deceased and the circumstances of death, where appropriate;

- For the purpose of legal proceedings, in specific circumstances;

- For the purpose of research, provided that specific requirements regarding the preparation of a research plan, approval by a research ethics board, and an agreement between the Health Information Custodian and the researcher, as outlined in PHIPA, are met;

- For any purpose as required or permitted by law.

3.1 – Disclosure of Information for Health Care Purposes

Express Consent - Should an individual wish his or her other health care providers working externally to the College Health Services to have access to the health Record, the individual can provide a written statement of consent to this effect.

The following is the process for releasing health Records to a third-party relying on an individual's express consent:

1. Record the date of the request in the health Record:

2. Advise the individual's primary health care provider of the request.

3. If the written statement of consent to the third-party organization is authorized by the College:

    a. Select and photocopy/print requested specific information;

    b. Do not photocopy/ print the entire health Record unless required;

    c. Prepare an official cover letter that will accompany the released information;

    d. Send out/mail out requested information;

e. Scan the letter of request, individual's consent, and a copy of the covering letter and save in the individual's health Record;

f. Costs associated with release of information will be invoiced by the College.

4. If the request is incomplete, unclear or contains an invalid consent or is otherwise not authorized by the College:

a) Inform the individual who made the request of the problem in writing (or in person or by phone as appropriate), such as:

1. The request is not sufficient to identify the individual;

2. The request is unclear or unspecific;

3. The request does not have the required consent;

4. The date the individual's consent was signed is greater than 90 days from the date the request was received.

b) Document the date, time of the call, name of the person with whom contact was made, a brief summary of the conversation and comments made by the requester.

Implied Consent – Circle of Care - The College may also disclose Personal Health Information to the individual's other health care providers for health care purposes (within the "**circle of care**") **without the express written consent** of the individual as long as it is reasonable in the circumstances to believe that the individual wants the information shared with other health care providers. However, no information will be released to other organizations if the individual has stated they do not want the information shared.

The following is the process for disclosing health Records to a third-party health care provider relying on an individual's implied consent:

1. Record the date of the request in the health Record

2. If disclosure of information to the third-party health care provider is authorized by the College:

a) Select and photocopy/print requested specific information;

b) Do not photocopy/print the entire health Record unless required;

c) Prepare an official cover letter that will accompany the released information;

d) Send out/mail out requested information;

e) Record the verbal request for information;

f) Costs associated with release of information will be invoiced by the College.

3. If the request is incomplete, unclear or the College has been advised by the individual not to disclose relying on implied consent, or the request is otherwise not authorized by the College:

    a) Inform the requester of the problem in writing (or in person or by phone as appropriate), such as:

        - The request is not sufficient to identify the individual;
        - The request is unclear or unspecific; and / or
        - The request does not have the required consent

    b) Document the date, time of the call, name of the person with whom contact was made, a brief summary of the conversation and comments made by the requester.

3.2 – Disclosure of Personal Health Information to Third Parties

If an individual wishes his or her lawyer, insurance company, employer, landlord or other such persons or agencies to have access to his or her Personal Health Information, the individual **must provide a written statement of consent to this effect**, which will be directed to the College.

The College will not process verbal third-party requests for release of information to anyone who is not a health care provider. These requests must be in writing. No information will be released without the express consent from the individual or the authorized person (unless permitted or required by law). See below "**Permitted or Mandatory Disclosures of Information**"). Third party requests not accompanied by appropriate consent will be returned with an official letter, outlining proper and complete consent requirements.

Any third-party request for disclosure of information shall include:

1. The name, address and telephone number of person or agency requesting the information.

2. The full name, address and date of birth of the person about whom the information relates.

3. A specific description about the type and amount of information to be released.

4. A consent for release of information form signed by the individual (or individuals authorized person or substitute decision-maker) and this consent form must not be older than 90 days from the date of the request.

The following is the process for disclosing health Records to a third party with consent of the individual to whom the PHI relates:

1. Record the date of the request in the health Record.

2. If the disclosure of information to the third party is authorized by the College:

    a) Select and photocopy/print requested specific information.

    b) Do not photocopy/print the entire health Record unless required.

    c) Prepare an official cover letter that will accompany the released information.

    d) Send out/mail out requested information.

    e) Scan the letter of request, consent, and a copy of the covering letter and save in the individual's health Record.

3. If the request is incomplete, unclear or contains an invalid consent or is otherwise not authorized by the College:

    a. Inform the requester of the problem in writing (or in person or by phone as appropriate), such as:

        - The request is not sufficient to identify the individual;

        - The request is unclear or unspecific;

        - The request does not have the required consent;

        - The date the individual's consent was signed is not recent; while legally still accurate, the College may ask why it has taken a length of time for it to be provided.

    b. Document the date, time of the call, name of the person with whom contact was made, a brief summary of the conversation and comments made by the requester.

Notification to Police

The College's cooperation with the police and assisting them in their investigations must be balanced against an individual's right to privacy and the right to confidentiality of their Personal Health Information.

The fact that an individual is suspected of being a victim of a crime or suspected of having committed a crime is not a recognized reason for breaching the individual's right to confidentiality. However, there is a recognized exception ("**discretion to warn**") to the individual's confidentiality where there is a significant risk of serious bodily harm to someone (either the individual or someone else) **and if it is genuinely believed that disclosing information to police could eliminate or reduce that risk.**

Personal Health Information will only be released to police upon the presentation of one of the following documents:

- A consent for release of information form signed by the individual or authorized person;

- A valid court order (or other legal document) requiring the release of information to the police; or

- A coroner's writ requiring the release of information to the police.

Each document must be reviewed carefully before information may be disclosed to police to ensure the disclosure is **permitted or required** by law.

This review should be done by appropriate staff, such as the individual's health care provider, a Privacy Office and/or Legal Services before any information is released. The documentation from the individual, police, court or coroner will be scanned into the chart. Legal advice should be sought as necessary.

Notification to Regulatory Colleges

Under the *Regulated Health Professions Act, 1991* and other health profession specific legislation, regulatory colleges may have the authority to review individual Records as part of investigations or quality assurance practices. Any documentation from a regulatory college claiming legal authority to require the release of information by the college must be reviewed carefully before information may be disclosed (for the section of the legislation giving the legal authority that the release of information is **permitted or required** by law). This review should be done by the Privacy Office and/or Legal Services before any information is released. The documentation from the regulatory college will be scanned into the Records.

Notification to Other Authorities

Certain legislation gives government agencies and others authority to review individual Records (such as immigration, the Ministry of Health, workplace safety and insurance and others). Any documentation from an agency claiming legal authority to release information to the agency must be reviewed carefully before information may be disclosed (for the section of the legislation giving the legal authority that the release of information is **permitted or required** by law). This review should be done by the Privacy Office and/or Legal Services before any information is released. The documentation from the agency requesting the information will be scanned into the Records.

Notification to Lawyers

Most lawyers' letters require individual consent for the release of information to a lawyer. The College must not release information to a lawyer without the individual's written consent unless the College has some other documentation to state that the College is required by law to disclose the information. Any documentation from a lawyer claiming legal authority to release information to the lawyer must be reviewed carefully before information may be disclosed. This review should be done by the Privacy Office and/or Legal Services before any information is released. The documentation will be scanned into the Records.

Permitted or Mandatory Disclosure of Information

The College may disclose Personal Health Information about an individual as permitted or required by law such as the *Health Care Consent Act, 1996, Regulated Health Professions Act,*

Ontario College of Social Workers and Social Service Workers Act; Child, Youth and Family Services Act, 2017, and *FIPPA.* These disclosures must be reviewed on a case by case basis, and the Privacy Office should be contacted for further information.
Please note that just because a disclosure is permitted, it does not mean that it is mandatory unless it is necessary to carry out a statutory or legal duty. For example, the *Health Protection and Promotion Act* requires Health Information Custodians to report all communicable diseases to the Medical Officer of Health. Reporting is done by the individual's health care provider or delegate as soon as possible after the diagnosis is made.

Disclosure for Fundraising Activities

Please contact the Privacy Office if your department wishes to use Personal Health Information for fundraising, which is subject to various requirements.

4.0 – Retention of Personal Health Information

Records containing Personal Health Information must be retained in accordance with the following retention table:

Information Type	Retention Period
Paper Records	*Adult patients*:*10* years from the date of the last entry in the record; *Patients who are children*: 10 years after the day on which the patient reached or would have reached 18 years of age.
PHI in any Electronic System	*Adult patients*:*10* years from the date of the last entry in the record; *Patients who are children*: 10 years after the day on which the patient reached or would have reached 18 years of age.
Archival copies of Electronic Records	*Adult patients*:*10* years from the date of the last entry in the record; *Patients who are children*: 10 years after the day on which the patient reached or would have reached 18 years of age.
Backups of any electronic system, audit logs or reports	The longer of 30 years or when any stored PHI has been destroyed/disposed of.
Audit logs containing PHI	The longer of 30 years or 15 years after any stored PHI has been destroyed / disposed / removed from the audit log.
Information about an Individual if related to an Access Request or Correction Request, or an inquiry	2 years after the Request for Access / Correction / inquiry has been completed.
Information about an Individual in relation to complaint or privacy breach	2 years after the Complaint or Privacy Breach has been closed by the HIC, Fleming College, or the Information and Privacy Commissioner of Ontario, whichever is longer.

If the College wishes to outsource the storage of Personal Health Information to a service provider whether in Ontario or another jurisdiction, the College must ensure that the service provider, who is acting as an Agent on behalf of the College, has the appropriate administrative, physical and technical safeguards in place to protect the Personal Health Information. This is typically achieved via a written agreement with the Agent.

5.0 – Disposal of Personal Health Information

Secure Disposal of Paper Records

Paper Records must be disposed of by shredding the Record using a cross-cut shredder or by placing them in the appropriate secure bin for shredding. The College shall ensure that Records that are destroyed or disposed of cannot be reconstructed or retrieved. Department Heads are responsible for determining methods of destruction and disposal that merit a certificate of secure destruction.

Secure Disposal of Electronic Records

If the Record is in electronic format, the Personal Health Information must be adequately deleted without being retrievable or reconstructable. When a Record in electronic format that contains Personal Health Information reaches the end of its lifecycle, it should be provided to ITS for secure data destruction.

ITS will follow secure data destruction procedures that comply with PHIPA and its regulation:

- For devices encrypted with strong encryption, full destruction/overwrite of all device decryption keys will be performed, e.g. secure wipe device to clear secure enclave.
- For magnetic media destruction (data tapes and drives), ITS will use a degausser which is fully certified to all major certifications: NIST 800-88, PCI, HIPAA, PIPEDA.
- For non-magnetic media when software over-write is required, software tools must be either NIST 800-88 or DoD 5220.22-M (7-pass) compliant.
- A certified eWaste vendor to perform physical item destruction may also be used. In this case, a certificate of secure destruction for each item with serial number is required.

Destruction Logs

Upon disposal or destruction of Personal Health Information, the College must log the date and type of Record that was destroyed, or disposed of, how, and by whom. Department Heads are responsible for maintaining these logs. Destruction logs must not contain any Personal Health Information.

When an ITS employee is enlisted to securely dispose of an electronic Record of Personal Health Information, that employee is responsible for providing verification of destruction of the electronic Record to the appropriate Department Head. This verification must include the date and type of Record that was destroyed or disposed of, how, and by whom. The Department Head will enter this information into the destruction log.

When destruction is performed by a third-party service provider, a certificate of secure destruction is required. The Department Head is responsible for tracking certificates of secure destruction in the destruction log and filing copies of certificates of destruction in a restricted electronic folder.

Destruction logs may be audited by the College at any time.

6.0 – Privacy Office and Legal Services

In certain circumstances, the College may not be certain if information can be used or disclosed. For example, if the College is uncertain if certain types of Personal Health Information may be used or disclosed without consent, it should contact the Privacy Office. Legal Services may also be consulted. If there any questions about this procedure, please contact the Privacy Office.

7.0 – Compliance and Enforcement

Compliance with the College's policies and procedures is subject to audit and review. Suspected violations should be reported to the appropriate authorities. The information will be reviewed by the appropriate authorities, including Human Resources, as required. Violations due to human error or operational procedure gaps or deficiencies will be addressed through training modifications to procedures, as required. All other violations may be subject to a range of disciplinary actions, including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with the College.

8.0 – Related Documents

- Information Practices Related to Personal Health Information Policy
- Collection of Personal Health Information Procedure
- PHIPA Request Form
- *Personal Health Information Protection Act, 2004* S.O. 2004. c.3 Sched. A. https://www.ontario.ca/laws/statute/04p03
- IPC Fact Sheet: Secure Destruction of Personal Information https://www.ipc.on.ca/wp-content/uploads/Resources/fact-10-e.pdf
- https://www.ipc.on.ca/health-organizations/collection-use-and-disclosure-of-personal-health-information/disclosure/

9.0 – History of Amendments & Reviews

Approved by SMT February 24, 2021