Fleming College

Policy Title:	Health Privacy Breach Procedure
Policy ID:	#1-112C
Manual Classification:	Section 1 – College Policies
Linked to Policy:	Information Practices Related to Personal Health Information
Approved by Board of Governors:	Original: March 25, 2020
Revision Date(s):	N/A
Effective Date:	March 25, 2020
Next Policy Review Date:	March 2023
Contacts for Policy Interpretation:	Policy and Privacy Coordinator Privacy Officer (to be hired) Manager of Operations - President's Office

1.0 – Purpose

The purpose of this procedure is to enable a quick and coordinated response to a Privacy Breach of Personal Health Information, to clarify roles and responsibilities, to establish a process to investigate, contain and remediate the breach and to prepare for possible involvement of the Ontario Information and Privacy Commissioner.

Some steps may have to be followed or implemented before other steps, for example, you may need to investigate the nature and scope of the breach in order to make an initial report. It is important to act immediately, to review and if necessary, repeat some of the steps below.

Capitalized words not defined here, are defined in #1-112 Information Practices Relating to Personal Health Information Policy.

2.0 – Application of Procedure

This procedure applies to all members of the College Community and Agents that handle Personal Health Information on behalf of the College.

Under PHIPA the College is a Health Information Custodian in respect of the following 3 health services: (1) Counselling Services (2) Student Health Services and, (3) the Massage Clinic (each a "**College Health Service**" and collectively the "**College Health Services**"). Capital terms not defined in this Procedure have the same meaning found in the College's policy about Information Practices Related to Personal Health Information.

3.0 – Definitions

"**Privacy Breach**" covers every instance of theft, loss unauthorized access, or unauthorized disclosure or destruction of PHI. Examples of privacy breaches include:

a) Loss or theft of portable devices containing PHI;

b) Misdirected faxes (or emails) containing PHI;

c) Cyberattacks, including ransomware attacks on records of PHI;

d) Deliberate unauthorized access to health records or PHI; and / or

e) Release or handling of PHI in a manner that is inconsistent with the law

4.0 – Responsibility for Notification

All members of the College Community and College Agents are responsible for ensuring the security and confidentiality of Personal Health Information held by the College. You must review, understand and follow the College privacy policies and procedures and your Department's specific processes.

The Department Head(s) are each responsible for:

a) Notifying the Privacy Coordinator of all Privacy Breaches and suspected Privacy Breaches within their Department;

b) Working with staff in their own Department(s) to follow the steps in this procedure to enable timely reporting to the Privacy Coordinator;

c) Developing and implementing the Department's own privacy breach notification procedures that are consistent with PHIPA and this procedure;

d) Ensuring Department staff are trained on and comply with all required procedures;

e) Working with the Privacy Coordinator to contain any Privacy Breach and mitigate against future Privacy Breaches.

The Privacy Coordinator is responsible for:

a) Maintaining a log of Privacy Breaches;

b) Maintaining ongoing communication with Department Head(s) to support responses to Privacy Breaches;

c) Notification to individuals affected by any Privacy Breach;

d) Notification to the IPC of Privacy Breaches, in consultation with other Departments, senior management and/or legal counsel, as may be necessary; and

e) Reporting Privacy Breach statistics to the IPC

4.1 – STEP 1: Notification within the College

1. Immediately upon learning of a privacy breach, notify your immediate supervisor(s) who in turn shall notify the applicable Department Head. The Department Head is responsible for notifying the College Privacy Coordinator.

2. The Department Head is responsible for notifying the College Privacy Coordinator as soon as reasonably possible after discovering or being notified of the breach.

3. The following information should be given to the Privacy Coordinator when notifying:

    a) Where appropriate, the name(s) of the Agent(s) or member(s) of the College Community responsible for the breach;

    b) The date of the breach;

    c) A description of the nature and scope of the breach;

    d) A description of the PHI that was subject to the breach **(*not the PHI itself*).**

4. Depending upon the nature and seriousness of the breach, the Department Head, together with the Privacy Coordinator, shall consider contacting the appropriate, senior manager(s).

5. If the breach involves an electronic health record system that is shared between two or more Health Information Custodians, the Privacy Coordinator shall notify the other custodians.

4.2 – STEP 2: Containing the Breach

1. The department head and privacy coordinator, in conjunction with the appropriate staff shall identify the individuals and organizations who are involved with or affected by the breach. This is likely one or more of the College Health Care Services. It may also include employees and Agents of the College and patients of the Health Care Services.

2. If possible, retrieve and secure any PHI that was disclosed improperly.

3. Make sure that no copies of disclosed PHI were made or retained by a person who was not authorized to receive that PHI. Record the contact information of all unauthorized recipients of improperly disclosed PHI; that contact information may be needed for follow-up.

4. If the breach involved an electronic health records system, or a system shared between one or more Health Information Custodians, and there is a danger of additional unauthorized access to or disclosure of PHI, change passwords and identification numbers, and if possible and necessary, temporarily shut down the system.

5. If the breach occurred due to a member of the College Community improperly accessing PHI, consider suspending that individual's access rights both in the short term, and in the long-term, in accordance with the outcome of any College investigation or proceeding.

4.3 – STEP 3: Third-Party Notification

1. **Notify Affected Individuals.** PHIPA requires that the College notify individuals affected by the breach at the first reasonable opportunity. The Privacy Coordinator shall coordinate the notification process, ***not*** the Department Head(s).

   Notification may be written or oral or a notation may be made in the patient record to discuss the breach at the next appointment. The College will inform the affected individual about the breach and that he or she has a right to make a complaint to the Information and Privacy Commissioner of Ontario ("**IPC**"). If the breach included disclosure of individuals' Ontario Health Card Numbers, individuals will be notified as follows:

   If your health card number has been affected by the breach, you should call ServiceOntario INFOline at 1-866-532-3161 or 1-800-387-5559 to report your lost or stolen health card number. If you suspect misuse of your health card number, you can report suspected cases of fraud by calling the Ministry of Health at 1-888-781-5556 or e-mail at reportohipfraud@moh.gov.on.ca.

2. **Notify the IPC (discretionary).** The Privacy Coordinator, on behalf of the College, may contact the IPC if notification of the affected individuals is not possible, if the College is unsure as to the best method of notification (likely due to the sensitivity of the PHI), or to discuss possible notification methods. In some cases, notification may be detrimental to the individual and the Privacy Coordinator may call the IPC to discuss. Legal counsel may also be consulted.

3. **Notify the IPC (mandatory**); The Privacy Coordinator, on behalf of the College, is mandated to notify the Commissioner of the theft, loss or unauthorized use or disclosure of PHI in the following circumstances:

   a) The College has reasonable grounds to believe that:

      - The unauthorized use or disclosure of PHI occurred by a person who knew or ought to have known that they were using or disclosing the information without authority;
      - PHI was stolen;
      - After an initial loss, or unauthorized use or disclosure, the PHI was or will continue to be used or disclosed without authority;
      - The loss or unauthorized use or disclosure of personal health information is part of a pattern of similar losses or unauthorized uses or disclosures.

   b) The College employs or engages a regulated health professional (likely in one of the College Health Services) and is required to give notice to a health profession regulator regarding a loss or unauthorized use or disclosure of PHI involving that professional. (see paragraph 4, below)

c) The College determines that the theft, loss or unauthorized use or disclosure of PHI is significant after considering all of the following that are relevant:

- It is sensitive PHI.
- The breach involved a large volume of PHI.
- The breach involved the PHI of many individuals.
- More than one Health Information Agent or Custodian was responsible for the breach.

The Privacy Coordinator is responsible for annual reports to the IPC that include privacy breach statistics. The College must keep statistics about the number of breaches involving lost PHI, stolen PHI and PHI that was used without authority and disclosed without authority. For additional details about PHI that must be kept for annual privacy breach statistical reporting to the IPC visit the IPC website or contact the Privacy Coordinator.

4. **Notify the Health Profession Regulatory College(s).** You are required to notify a health care practitioner's regulatory college within 30 days if any of the following applies:

a) The health care practitioner was an employee or of the College and the employment or affiliation was terminated, suspended, or subject to disciplinary action as a result of a Privacy Breach.

b) The practitioner resigns or relinquishes his affiliation with the College and the College has reason to believe that the resignation or relinquishment relates to an investigation or other action carried out by the College as a result of an alleged Privacy Breach.

5. Information to Include in the Notice

The following information should be included in the notice:

a) Where appropriate, the name of the Agent or member of the College Community responsible for the unauthorized access (This information may only be required for notifying within the College, and only in limited situations);

b) The date of the breach;

c) A description of the nature and scope of the breach;

d) A description of the PHI that was subject to the breach;

e) The measures implemented to contain the breach;

f) The name and contact information of the person in your organization who can address inquiries (the College Privacy Coordinator); and

g) Whether the IPC was notified of the breach.

Note: If you are a custodian who is a researcher and have received personal health information for research purposes from another custodian, you must not notify an individual about whom the personal health information relates, unless you are informed that the individual has given consent to being contacted

4.4 – STEP 4: Investigation, Remediation and Recording

1. The Privacy Coordinator will coordinate and conduct an internal investigation to ensure the breach is contained, and this response procedure has been implemented.

2. The investigation will include, but is not limited to: reviewing the circumstances surrounding the breach, reviewing the privacy and security policies and protocols to ensure they are adequate to protect the College's PHI (and planning to amend if necessary), determining whether systemic issues need updating (for example, updating technological systems).

3. Correspond with the IPC if you notified IPC of the breach. If the IPC is investigating the breach, cooperate with the IPC.

4. Keep a log of all privacy breaches. Privacy breach statistics must be reported to the IPC annually. The log must contain the following information:

    a) The name of the employee or Agent that caused the breach, where it is determined to be relevant, such as in the case of unauthorized access;

    b) The date of the breach;

    c) The nature, scope and cause of the breach;

    d) The number of individuals affected by the breach; and

    e) A description of the PHI that was subject to the breach, and o a summary of the steps taken to respond to the breach. For more information about the information that must be logged, tracked and reported to the IPC visit the IPC website or contact the Privacy Coordinator.

4.5 – STEP 5 (if applicable): IPC Correspondence

When investigating a privacy breach, the IPC may, depending on the circumstances:

1. Ensure any issues surrounding containment and notification have been addressed;

2. Interview individuals involved with the privacy breach or individuals who can provide relevant information;

3. Receive representations from individuals whose privacy has been breached;

4. Obtain and review your position on the privacy breach;

5. Ask for a status report of any actions that you have taken;

6. Review and provide input and advice on your current information management policies and procedures; and / or

7. Issue a *PHIPA* Decision that may contain recommendations and/or orders that require proof of compliance.

5.0 – Accountability

1. The College will inform individuals who make a request related to this procedure of their right to appeal any decision of the College with respect to their request to the Information and Privacy Commissioner of Ontario.

2. The College will provide training to its employees and agents to ensure compliance with this procedure and all related policies.

3. Any suspected or confirmed breaches of privacy must be immediately reported in accordance with this Health Privacy Breach Procedure.

4. The College will review this procedure annually.

5. College employees and Agents who fail to adhere to this procedure may be subject to disciplinary action by the College.

6.0 – Related Documents

- Information Practices Relating to Personal Health Information Policy
- Student Code of Conduct
- *Personal Health Information Protection Act, 2004*
- IPC Documents:
    - Responding to a Health Privacy Breach: Guidelines for the Health Sector. OPIC. October 2018: https://www.ipc.on.ca/wp-content/uploads/2018/10/health-privacy-breach-guidelines.pdf

7.0 – History of Amendments & Reviews

Section(s)	
Date / Creator	