Policy Title:	Privacy		
Category:	☐ Institutional - Board ☒ Institutional - Administrative	☐ Academic - Administrative ☐ Employment - Administrative	
Approved by:	☐ Board	☒ President	
Date approved:	August 30, 2018	**Effective date:**	August 30, 2018
Policy Sponsor:	Chief Privacy Officer	**Date last reviewed:**	August 30, 2018
Date of Mandatory Review (expiry date)	August 2023	**Date of last revision of Procedures**	August 2019

1 POLICY

1. Personal information is collected in a lawful and fair manner that is not unreasonably intrusive. Wherever possible, personal information is collected directly from an individual. CMCC collects personal information only for the following purposes:

    a. to provide products and perform services expected by our students, patients, alumni, customers, as set out in contractual obligations with them

    b. to understand customer needs

    c. to develop, enhance, market or provide services or products

    d. to meet legal and regulatory requirements.

2. CMCC will not use any personal information for any purposes other than those for which it is collected except with the consent of the individual or as required by law. CMCC retains personal information only as long as necessary for the fulfillment of those purposes, or as required by law.

3. CMCC will ask an individual to specifically consent to the collection, use, or disclosure of their personal information. Normally, consent is obtained in writing, but oral consent may be accepted under certain circumstances. For non-sensitive personal information, consent may also be implied when reasonable. An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.

4. All reasonable precautions will be taken to ensure that personal information is kept safe from loss, unauthorized access, modification or disclosure. CMCC protects personal information with security safeguards appropriate to the sensitivity of the information. Only persons whose duties reasonably so require are granted access to personal information.

5. CMCC takes reasonable steps to ensure that personal information is protected when shared with service providers. Due to CMCC's service provider relationships, personal information may be processed and/or stored in a foreign country where it may be accessible to law enforcement and national security authorities of that jurisdiction.

6. CMCC shall not use or disclose for any new purpose personal information that has been collected without first identifying the new purpose and obtaining the consent of the individual or as may be required by law.

7. Personal information will be disclosed under the following circumstances:

    a. when consent to the disclosure is received. In such cases the person receiving the request for disclosure shall determine whether the consent is in compliance with CMCC policy on releasing the information prior to any disclosure. This may include release of health care records to law firms or other health care practitioners, as well as student or employee information.

    b. when required or authorized by law to do so, for example if a court issues a subpoena or in an emergency. All subpoenas shall be referred to the Chief Health Records Custodian for health information, Registrar for student information, or in all other cases, the Chief Privacy Officer (CPO).

    c. when the services provided to an individual require CMCC to contractually give information to third parties (for example, for the student health plan) consent will be implied, unless specified otherwise.

    d. where it is necessary to establish or collect fees.

    e. where CMCC engages a third party to provide administrative services (like computer back-up services or archival file storage), the third party is contractually obligated to adhere to this Privacy policy.

    f. when CMCC engages lecturers on a contract basis for the purposes of conducting such lectures.

    g. when undergoing an accreditation, audit and/or review process.

    h. for the purposes of continuing to carry out the services provided.

    i. if the information is publicly available and is being disclosed for purposes consistent with the purposes for which it has already been published.

    j. as required for investigation of any breach of CMCC policy or procedure.

8. It is the individual's responsibility to provide CMCC with the information necessary to ensure that their records are correct.

9. Upon request, an individual shall be informed of the existence, use and disclosure of their personal information and shall be given access to that information. An individual may challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Any complaints or concerns about privacy are to be directed to CMCC's CPO and, in the case of personal health information, to the Chief Health Records Custodian.

11. Any individual becoming aware of a breach or suspected breaches of data/privacy must follow the Data Breach Response Procedure, after first notifying the CPO.

12. All privacy breaches will be logged by the Chief Privacy Officer and, for breaches of personal health information, by the Chief Health Records Custodian, in accordance with the procedures set out in CMCC's Privacy Breach Response Procedure (Attachment).

2 PURPOSE

To ensure accountability and adherence to the provincial and federal laws dealing with privacy of personal information, and to provide guidance on all reasonable steps necessary to limit, to the extent possible, substantial harm or inconvenience to individuals whose personal information has been compromised.

3 SCOPE

Employees, students, contractors provided access to personal information to carry out their duties, and volunteers at CMCC.

4 INFORMATION AND COMPLIANCE PLANS (not a comprehensive list)

CMCC is responsible to protect any personal information, including Personal Health Information, it collects and stores from a number of constituencies while ensuring that matters of privacy are adhered to and recognized.

General Data Protection Regulation (GDPR) Compliance

EU data subjects permanently residing in the European Union may have supplementary statutory rights with respect to their personal data as outlined in the *General Data Protection Regulation* EU/2016/679. This includes the right to have personal data deleted or object to/restrict processing of such data. If such a request is received, it should be immediately directed to the CPO. In the context of a request for erasure, CMCC will scramble or pseudonymize the data subject's information to make it anonymous.

CMCC is a Canadian organization and uses data hosting providers who have made GDPR commitments of their own. Canada was the first country outside of Europe deemed adequate by the EU Commission in 2001, under the EU Data Protection Directive 95/46/EC (the GDPR's predecessor). An adequacy finding allows the flow of data from the EU to Canada as a trusted country in data protection.

The following resources are available for further information on privacy expectations at CMCC:

- Chiropractic Act of Ontario, S.O. 1991, C. 21
- Clinicians' Manual
- Employee and Intern Online Training Modules – PIPEDA and PHIPA
- Health Information Protection Act, 2016 (HIPA)
- Information and Privacy Office of Ontario: Annual Reporting of Breach Statistics to the Commissioner – November 2017.
- Information and Privacy Office of Ontario: Reporting a Privacy Breach to the Commissioner – Guidelines for the Health Sector – September 2017.
- Personal Health Information Protection Act, 2004 (PHIPA)
- Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA)
- Regulated Health Professions Act of Ontario, S.O. 1991, C. 18

5 RELATED POLICIES (not a comprehensive list)

- Access to Student Information, Third Party
- Interns' Manual
- Record Management, Retention and Destruction
- Research Manual (Section D: Ethical Norms)
- Website Access, Use and Maintenance

6 DEFINITIONS

Chief Health Records Custodian is the person within CMCC responsible for overseeing the custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties.

Chief Privacy Officer (CPO) is the person within CMCC responsible for ensuring compliance with privacy obligations.

Personal health information is personal information in any form that identifies a person and that relates to their health and health care, including health history, health care programs and services, health care providers, substitute decision-makers, health card number and other personal identification numbers.

Personal information is information (in any form) that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Privacy breach (data breach) refers to any loss of, unauthorized access to, or unauthorized disclosure of personal information, whether identified internally or externally. A privacy breach may be a consequence of faulty business procedures, lack of a security safeguard, operational break down or human error.

New Policy Approved (date):
October 2003
Policy Revision History (dates):
June 1, 2017
May 31, 2018
August 30, 2018

----------**END OF POLICY**----------

7 PROCEDURES

1. On matters pertaining to the nature of disclosing information that may be considered personal, employees should seek clarification from their manager and, if appropriate, the Chief Privacy Officer (CPO).

2. Any individual may make a written request for access to their personal information held by CMCC. Requests must be approved as per policy. Requests for more detailed information requiring archival or other retrieval may be subject to reasonable professional and disbursement fees.

3. CMCC will promptly deal with an application to amend any personal information and if found to be inaccurate or incomplete, such information shall be amended. Individuals having any questions, or wishing to access personal information, are to write to:

   Chief Privacy Officer
   Canadian Memorial Chiropractic College
   6100 Leslie Street
   Toronto, ON M2H 3J1

4. All incidents pertaining to a breach of privacy shall be documented (for archival and follow up purposes) on a Privacy Incident Report form, available on MyCMCC and S:\CMCC-Public.
5. In order to ensure a consistent and compliant approach to the handling of all privacy breaches, CMCC has developed, as a separate procedure, a Privacy/Data Breach Response Procedure to be followed in the event of a breach.

6. On or before March 1 in each year, the Chief Health Records Custodian shall provide the Information Privacy Commissioner with a report setting out the number of times in the previous calendar year that a privacy breach occurred in each of the following categories:

   a. Personal health information in the custodian's custody or control was stolen.

   b. Personal health information in the custodian's custody or control was lost.

   c. Personal health information in the custodian's custody or control was used without authority.

   d. Personal health information in the custodian's custody or control was disclosed without authority.

New Procedure Approved (date):
October 2003
Procedure Revision History (dates):
June 1, 2017
May 31, 2018
August 2019

8 ATTACHMENTS

Privacy Breach Response Procedure

Attachment

PRIVACY BREACH RESPONSE PROCEDURE

DEFINITIONS

Personal information: Any information about identifiable individuals, such as applicants, students, alumni, patients, research subjects, customers, employees, volunteers or other representatives of CMCC.

Privacy Breach (Data Breach): Any loss of, unauthorized access to, or unauthorized disclosure of personal information, whether identified internally or externally. A privacy breach may be a consequence of faulty business procedure, lack of a security safeguard, operational break-down or human error.

Significant Harm: Bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

PROCEDURE OBJECTIVES

This Procedure has been adopted to allow for prompt and reasonable action by CMCC in the event of a Privacy Breach. It will provide guidance on all reasonable steps necessary to limit, to the extent possible, substantial harm or inconvenience to individuals whose personal information has been compromised.

CMCC shall ensure a consistent, compliant approach to the handling of all privacy breaches. Each department of CMCC is responsible for integrating this Policy into its operations and incident response programs. Upon identification of a privacy breach, the Vice President, Administration and Finance (also CMCC's Chief Privacy Officer) must be immediately notified.

STEPS FOR RESPONDING TO A PRIVACY BREACH

1. Breach Containment and Preliminary Assessment

Immediate common sense steps will be taken to limit the breach and its consequences, including:

- Contain the breach, e.g. put an end to the unauthorized practice, recover the records, shut down the system that was privy to the breach, revoke or change computer access codes or correct weaknesses in physical or electronic security.

- Designate an appropriate individual to lead the initial investigation. This individual should have appropriate authority within CMCC to conduct the initial investigation and make initial recommendations. If necessary, a more detailed investigation may subsequently be required.

- Determine who needs to be made aware of the incident internally and externally. Inform CMCC's Privacy Officer of the breach.

- Determine the need to assemble a team comprised of representatives from appropriate parts of the business.

- If the breach is deemed to involve theft or other criminal activity, police shall be notified

- Ensure an investigation of the Breach is not compromised. Any and all evidence that is potentially valuable in determining the cause of the breach or that would allow CMCC to take appropriate corrective action must not be destroyed.

2. Evaluate Risks Associated with the Breach

The following factors will be considered in assessing the risks associated with the Privacy Breach:

(i) Personal Information Involved

- Determine whose information has been compromised by the breach and the type of personal information compromised.

- Assess the nature and scope of the breach and identify the level of sensitivity of personal information compromised. Some information is considered more sensitive than others, e.g. health information, social insurance numbers, driver's licenses, health card numbers, credit or debit card numbers. The greater the level of sensitivity, the greater the risk of harm to individuals.

- Determine if the personal information is adequately encrypted, anonymized or otherwise not easily accessible.

- Assess the manner in which the personal information can be used, e.g. can the information be used for fraudulent or otherwise harmful purposes? The combination of certain types of sensitive personal information along with name, address and date of birth suggest a higher risk due to the potential for identity theft.

(ii) Cause and Extent of the Breach

- To the extent possible, determine the cause of the Privacy Breach

- Evaluate if there is a risk of ongoing breaches or further exposure of the information

- Determine the number of individuals whose personal information was affected by the breach

- Establish the extent of the unauthorized access to or collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure, including via mass media or online.

- Determine if the information was lost or stolen. And, if stolen, whether it was the target of the theft in question
- Inquire as to whether compromised personal information has been recovered

- Consider whether the breach can be deemed a systemic problem or an isolated incident

(iii) Foreseeable Harm from the Breach

- In assessing the possibility of foreseeable harm from the breach, consider an individual's reasonable expectations.

- Determine the recipient of the personal information (if possible) and whether a relationship exists between the unauthorized recipients and the subjects of the breach, i.e. evaluate if the recipient is a trusted and known entity who can reasonably be expected to return information in question without disclosure or use.

- Evaluate the potential harm of the breach to individuals, e.g. security risk, identity theft, financial loss, loss of business or employment opportunities, humiliation, or damage to reputation or relationships.

- Assess the potential harm of the breach to CMCC, e.g. loss of trust, loss of assets, financial exposure or legal proceedings.

- Assess what steps, if any, have already been taken to mitigate the harm resulting from the breach.

3. Individual Notification

Based on the sensitivity of the information and the probability that the personal information has been, is being, or will be misused, determine if the Privacy Breach creates a **real risk of significant harm**. If so, individuals affected shall be promptly notified. In this way, individuals can take steps to protect themselves, mitigating any subsequent damage.

"Significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

Note however that in the context of CMCC clinics' patient data, under the Ontario *Personal Health Information Protection Act*, individuals must be notified if their personal health information has been lost, stolen or accessed by an unauthorized person irrespective of whether or not there is a risk of significant harm.

(i) Procedure to Notify Individuals

When to Notify: Once it is determined that notifying individuals is necessary**,** notification of those affected shall occur as soon as feasible after CMCC's Privacy Officer confirms the occurrence of the Privacy Breach and concludes that notification is required. However, if law enforcement authorities are involved, CMCC shall confer with those authorities to determine whether notification must be delayed to ensure the investigation is not compromised.

How to Notify: Upon identifying the individuals affected by the breach, CMCC's Privacy Officer must determine the appropriate manner of delivery of notification. Delivery may be made in any manner designed to ensure that an individual can be reasonably expected to receive it. The preferred method of notification is direct – by phone, letter, email or in person – to affected individuals. Indirect notification – website information, posted notices, media – should occur only where direct notification could cause further harm, is prohibitive in cost, or the contact information

for affected individuals is not known. Using multiple methods of notification in certain cases may be appropriate.

Who should Notify: The CMCC Privacy Officer will determine the most appropriate person to notify the affected individuals and may notify the affected individuals directly, even if the breach occurs at a third party service provider that has been contracted to maintain or process the personal information on behalf of CMCC. However, notification by a third party is sometimes deemed more appropriate, e.g. in the event of a breach by a retail merchant of credit card information, the credit card issuer may be involved in providing the notice since the merchant may not have the necessary contact information.

(ii) Content of Notification

The content of notifications will vary depending on the particular breach and the method of notification chosen. The notification must contain enough information to allow the individual to understand the significance of the breach to them and to take steps to mitigate that harm. The notice should include, as appropriate:

- A description of the incident and the date/time period of the incident
- A description of the personal information involved in the Privacy Breach
- A detailed outline of what CMCC has done to control or reduce the harm to individuals
- A description of how CMCC plans to assist individuals affected and what steps individuals can take to avoid or reduce the risk of harm. Possible actions include arranging for credit monitoring and terminating credit card account
- Contact information of a department or individual within CMCC who can answer questions or provide further information about the Privacy Breach

(iii) Others to Contact

(a) Privacy Commissioners and Data Protection Authorities: The Chief Privacy Officer will notify the federal privacy commissioner of the Privacy Breach as soon as feasible if there is a real risk of significant harm to individuals, or provincial privacy commissioners as required under applicable provincial privacy laws. All breaches of Personal Health Information must be reported to the Information and Privacy Officer of Ontario. A breach of an EU resident's personal data must be reported to the data protection authority of the relevant EU Member State within 72 hours of discovering the breach.

The following authorities or organizations may also be informed of the Privacy Breach:

(b) Police: If theft or other crime is suspected.

(c) Insurers: In order to file a claim to recover first or third party costs associated with a breach, it is often critical to report the breach to your insurance company as soon as possible.

(d) Professional or other regulatory bodies: if professional or regulatory standards require notification of these bodies.

(e) Credit card companies, financial institutions or credit reporting agencies: if their assistance is necessary for contacting individuals or assisting with mitigating harm (e.g. credit monitoring services).

(f) Other internal or external parties not already notified:

- CMCC's Board of Governors
- third party contractors or other parties who may be impacted; or
- other CMCC departments not previously advised of the privacy breach

4. Breach Recordkeeping

The following records will be maintained by CMCC's Privacy Officer and by the Chief Health Records Custodian, if a breach is of personal health information:

- Privacy Incident Report (*Attached)*
- Privacy Breach Response Procedures Form – Appendix A (*Attached*)
- Privacy Breach Log – Appendix B (*Attached*)

5. Prevention of Future Breaches

Once the appropriate steps to mitigate the risks associated with the breach are taken, CMCC will then consider a breach prevention plan. The decision shall be influenced by the significance of the breach and whether it was a systemic breach or an isolated instance. The plan may include the following:

- A security audit of both physical and technical security
- A review of policies and procedures and any changes to reflect the lessons learned from the incident and investigation (e.g., security policies, privacy policies, record retention policies, etc.)
- A review of employee training practices; and/or
- A review of service delivery partners