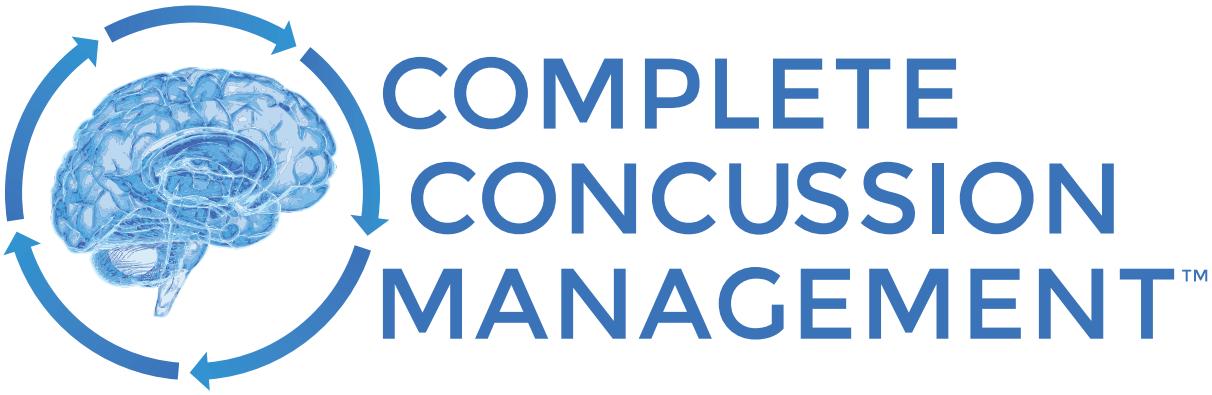

Health Information Network Provider (HINP) Privacy Policy

Document Control:	
Owned by:	Privacy Office
Implemented by:	December, 2017
Next Review Date:	December, 2019
Approved by:	Chief Privacy Officer
Effective Date:	January 1, 2018

For questions concerning this policy please contact:

CCMI Privacy Office

Complete Concussion Management Inc.

2655 Bristol Circle

Oakville, ON L6H 7W1

Email: privacy@completeconcussions.com

INTRODUCTION

Background and Overview

Complete Concussion Management Inc. ("**CCMI**") is a private full-service concussion management organization that is committed to providing the highest level of concussion care around the world. Founded in 2013, the CCMI network of licensed healthcare professionals provides concussion-related services to members of the general public through our proprietary electronic health portal (the "**CCMI Concussion Database System**") and related patient smartphone applications and healthcare portals.

As an international organization, CCMI:

- Provides educational programs for licensed healthcare professionals to improve their knowledge and expertise in the field of concussion management, treatment, and rehabilitation;

- Enters into partnership agreements with affiliated clinics who have licensed healthcare professionals who have successfully completed the CCMI practitioner certification course, and who hold a current standing with CCMI and their professional college or licensing body;

- Provides services related to the management and care of concussions by way of affiliated, community-based clinics;

- Uses the CCMI Concussion Database System to support licensed healthcare professionals, patient self-care, and to continually improve the safety, quality, efficiency, accessibility, and accountability of our concussion services;

- Provides secondary platforms to link various tools to the CCMI Concussion Database System in the form of patient and provider-facing smartphone applications (the "**CCMI Concussion Tracker***"*), as well as healthcare provider portals, utilized at the discretion of the patient, to improve communication throughout sporting, academic, vocational, and healthcare environments; and

- Rapidly disseminates research developments and innovation in clinical practice and concussion service delivery to our affiliated global clinical network.

In this pursuit, we are not only dedicated to utilizing the best scientific evidence to constantly evolve and develop our program; we are also committed to furthering research, academic/medical knowledge, concussion management, treatment, rehabilitation, education, and awareness about concussions and brain injuries. As such, we may collect a variety of information for the provision of our services and to further scientific research with respect to concussions. Some of the information CCMI collects is personal health information ("**PHI**") as defined by section 2 of the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"). Also, as we facilitate the electronic transmission of personal health information between healthcare providers,

we are a "health information network provider" governed by Ontario's *Personal Health Information Protection Act, 2004* ("**PHIPA**").

CCMI processes patient personal health information ("**PHI**") in two roles:

- A patient support role, in which CCMI deals directly with individual patients to support their use of the CCMI Concussion Tracker, and to facilitate (with patient consent) (i) the availability of their PHI to healthcare providers in CCMI's network of healthcare providers; and (ii) research; and
- A healthcare provider EMR role, in which CCMI facilitates the retention of PHI in electronic form on behalf of healthcare providers, and the transmission of PHI among healthcare providers.

Specifically, in these roles, CCMI uses the PHI it receives to:

- create and store pre-season baseline testing information for use in the event that an individual suffers a concussion;
- provide patient assessment, testing, referrals, and ongoing day-to-day patient care;
- provide communication lines between the patient's various healthcare providers;
- extract large-scale meta-data for the purposes of supporting health research;
- improve patient care; and
- provide communication to patients and their caregivers about the status of the patient's account, test expiration, health status, and general information that is necessary to their health.

PHI is disclosed by CCMI, as authorized by law and with patient consent, to organizations such as Clinical and Evaluative Sciences, the Canadian Institute for Health Information and Statistics Canada, as well as researchers who comply with the research requirements set out in PHIPA.

Finally, CCMI provides information technology ("**IT**") solutions, such as applications or network services, to health information custodians ("**HIC's**") involved in a number of health system programs and projects managed by CCMI.

Complete Concussion Management's Privacy Program

CCMI understands the importance of and is committed to respecting privacy, safeguarding confidential information and ensuring the security of PHI within its custody or control. CCMI meets this commitment through its Privacy Program. CCMI has implemented various safeguards to ensure the effectiveness of its Privacy Program, which includes appointing a Chief Privacy Officer ("**CPO**"), who manages the program and reports directly to CCMI's President & CEO. The CPO is supported in carrying out her responsibilities by a network of individuals and committees with specific privacy and security-related responsibilities, including:

- legal counsel with privacy and health privacy expertise;

- IT and development team responsible for designing secure infrastructure; and
- research coordinator who is responsible for determining and overseeing appropriate data extraction following the approval from a Research Ethics Board (REB)

Key components of CCMI's Privacy Program include:

- the CCMI Internal Privacy Policy and Procedures which guides our employees and personnel in their handling of PHI;
- an employee privacy training and awareness program;
- a privacy audit which monitors system access and patient file access; and
- a privacy impact assessment – underway

LEGISLATIVE AUTHORITIES

PHIPA establishes a statutory privacy framework for protecting PHI in Ontario. The Regulations[1] made under PHIPA specify further requirements for service providers to health information custodians (like clinics and individual physicians) ("**HICs**"), where those service providers enable those HICs to use electronic means to collect, use, modify, disclose, retain or dispose of PHI ("**Service Providers**").[2] The Regulations also specify requirements for "health information network providers" ("**HINPs**"), which are service providers that enable two or more HICs to use electronic means to share PHI with each other.[3]

CCMI provides IT services, such as the CCMI Concussion Database, to HICs to enable them to collect, use, disclose, retain or dispose of PHI. As such, CCMI is a Service Provider for the purposes of PHIPA. Service Providers are subject to the three privacy requirements found in section 6(1) of the Regulations, which include that the:

1. Service Provider's use of PHI is to be limited to that which is necessary to provide IT services;
2. Service Provider's disclosure of any PHI to which it has access in the course of providing the IT services is prohibited; and
3. Service Provider's employees or contracted third parties be limited to access only the PHI which is required to provide the IT services.

CCMI also provides information systems (listed in Appendix A) to HICs to enable them to exchange PHI with each other. In providing such services, CCMI is subject to additional privacy requirements under the PHIPA Regulations for HINPs, as specified below.

[1] Ontario Regulation 329/04.

[2] See section 10(4) of PHIPA and Section 6 of the Regulation to PHIPA.

[3] See section 6(2) of the Regulation to PHIPA.

SCOPE OF CCMI'S HEALTH INFORMATION NETWORK PROVIDER PRIVACY POLICY

CCMI's Health Information Network Provider Privacy Policy (the "**Policy**") applies to the provision of IT services by CCMI to two or more HICs, where the services are provided primarily to enable HICs to use electronic means to disclose PHI to one another. In addition to the Service Provider requirements outlined above, HINPs such as CCMI are subject to the requirements under section 6(3) of the Regulation to PHIPA.

This Policy describes the standards employed by CCMI to protect PHI managed in its capacity as a HINP and further describes how CCMI meets the privacy requirements as detailed in the Regulations.

This Policy is intended to supplement CCMI's Privacy Policy, which is the general framework document of CCMI's Privacy Program and describes the privacy practices CCMI employs to protect PHI.

This Policy and any amendments to the Policy are approved by the CPO. Amendments are communicated to CCMI staff, contracted third parties and participating HICs. Where appropriate, the Policy identifies supporting documents and relevant authorities for each of the fair information practices.

Where there is a discrepancy between this Policy and PHIPA, PHIPA takes precedence.

HINP Requirement 1: Breach Notification

CCMI will notify every applicable HIC, at the first reasonable opportunity, of any privacy breach, suspected privacy breach or privacy risk related to the unauthorized access, use, disclosure, or disposal of PHI managed by CCMI via its IT services.[4]

CCMI also requires that all employees and relevant third-party providers advise the CCMI Privacy Office at the first reasonable opportunity of any privacy breach, suspected privacy breach or privacy risk relating to the unauthorized access, use, disclosure, or disposal of PHI retained by CCMI or managed via its IT services. The terms "privacy breach", "suspected privacy breach" and "privacy risk" are defined and explained in CCMI's Privacy Breach Management Procedure.

The Privacy Office will notify the applicable HIC(s) Privacy Officer in writing immediately, upon any privacy breach, suspected privacy breach or privacy risk is identified.

See CCMI's Privacy Breach Management Procedure.

HINP Requirement 2: Providing HICs with a Plain Language Description of Services and Safeguards

[4] See section 6(3)(1) of the Regulation to PHIPA. 7

CCMI will supply each applicable HIC with a plain language description of the CCMI IT services provided and safeguards that have been implemented to protect PHI against unauthorized use or disclosure, and to protect the integrity of the information.[5]

CCMI's Privacy Office will ensure that the following are provided to each applicable HIC:

- general information on CCMI's Privacy Policy and practices;
- general information on CCMI's HINP Privacy Policy and related procedures;
- a description of the IT services provided as a HINP;
- a general description of the administrative, technical and physical safeguards in place to protect PHI in the information system(s); and
- contact information for CCMI's Privacy Office in order to facilitate HICs in making a request for information regarding CCMI's Privacy Program or practices

HINP Requirement 3: Public Description of Services, Safeguards, Directives, Guidelines and Policies

CCMI will make available, to the public, a plain language description of the CCMI IT services provided and the safeguards employed to keep PHI secure and confidential. This public description will include any directives, guidelines, and polices that apply to these services.[6]

CCMI's Privacy Office, in conjunction with CCMI's communications department, will ensure that the following are available to the public and key stakeholders.

- general information on CCMI's Privacy Policy and practices;
- general information on CCMI's Health Information Network Provider Privacy Policy and related procedures;
- a description of the IT services provided as a Health Information Network Provider;
- a general description of the administrative, technical and physical safeguards in place to protect PHI in the information system(s);
- contact information for CCMI's Privacy Office in order to facilitate public requests for information regarding CCMI's Privacy Program or practices

HINP Requirement 4: Provision of Access and Transfer Logs

CCMI will make available to the applicable HIC upon request, and to the extent reasonably practical, an electronic record of all accesses and transfers of PHI, associated with the HIC and held in equipment controlled by CCMI.[7]

[5] See section 6(3)(2) of the Regulation to PHIPA.

[6] See section 6(3)(3) of the Regulation to PHIPA.

[7] See section 6(3)(4) of the Regulation to PHIPA. 10

CCMI will make available to HICs upon request a list of the applicable access and transfer logs.

HICs may request such logs by contacting the CCMI Privacy Office via email (privacy@completeconcussions.com). Any logs for named patients (which contain PHI) may only be requested by telephone. The Privacy Office will only accept requests made by the HIC's Privacy Officer (or authorized delegate(s)).

Access and transfer logs sent by CCMI in response to a request for such logs will include the following:

- In the case of access logs:
    - The identity of the person who access the PHI; and
    - The date and time the PHI was accessed

- In the case of transfer logs:
    - The identity of the person who transferred the PHI;
    - The identity of the person to whom the PHI was transferred; and
    - The date and time the PHI was transferred

HINP Requirement 5: Providing HICs with a Privacy Impact Assessment and Threat Risk Assessment of Services Provided

CCMI will perform and provide to each applicable HIC a written copy of the results of a privacy impact assessment and threat risk assessment on the IT services provided.[8]

CCMI will conduct privacy impact assessments (PIAs) and threat risk assessments (TRAs) on all new or significantly amended CCMI IT services provided by CCMI in its role as a HINP. CCMI will share its PIAs with each applicable HIC.

Due to their sensitive nature, TRAs will be provided to the HIC's Privacy Officer or a senior security officer, subject to the signing of a non-disclosure agreement.

HINP Requirement 6: Restrictions on Employees and Third Parties

CCMI will ensure that all employees or contracted third parties retained comply with CCMI's privacy and security restrictions and conditions.[9]

The use of PHI contained in the information systems in CCMI's HINP role is restricted to CCMI staff and contracted third-parties that require access in order to support IT service provision.

To obtain access, CCMI staff and contracted third-parties are required to:

- sign a CCMI confidentiality agreement;

[8] See section 6(3)(5) of the Regulation to PHIPA

[9] See section 6(3)(6) of the Regulation to PHIPA.

- successfully complete privacy/security training, which describes the contents of this HINP Policy and associated procedures; and

HINP Requirement 7: Written Agreement with Respect to Services and Safeguards

CCMI will enter into a written agreement with each HIC describing the services provided, the administrative, technical and physical safeguards in place to protect the confidentiality and security of the information, and that requires CCMI to comply with PHIPA and its Regulations.[10]

The CPO will ensure that the services agreement includes the following restrictions:

- CCMI will not use PHI to which it has access in the course of providing IT services except as necessary in the course of providing the services;
- CCMI will not disclose PHI to which it has access in the course of providing IT services;
- All CCMI employees and contracted third parties agree to comply with CCMI's privacy and security requirements; and
- CCMI will notify the applicable HIC(s) at the first reasonable opportunity of any privacy breach, suspected privacy breach or privacy risk relating to the unauthorized access, use, disclosure or disposal of PHI. See CCMI's Privacy Breach Management Procedure.

[10] See section 6(3)(7) of the Regulation to PHIPA.

APPENDIX A: INFORMATION TECHNOLOGY SERVICES

This Appendix describes the information system(s) that Complete Concussion Management Inc. ("CCMI") provides participating health information custodians in its capacity as a Health Information Network Provider.

There are 3 branches of the system:

1) The CCMI Concussion Database System – this is the EMR that partnered clinics/clinicians use to record and track patient data
2) The Concussion Tracker app – used by coaches/ trainers to report injuries and follow progress of injured athletes. This also allows patients to input symptoms and get basic information about their condition, restrictions, and permissions at each stage of recovery – eventually we hope to be able to provide specific rehab exercises, track compliance, etc.
3) The Physician portal – these are not our partnered clinics but this is an access portal that a patient's family physician can use to check in on their patient. They can view and add notes on a patient's file but they are not the main custodian of that file. They enter in the person's account number, but as soon as they log out or leave that file, they would need the account number to get back in. In other words, no files are stored or accessible on the physician's portal. They can only search by entering account numbers.

CCMI Concussion Database System

CCMI provides the CCMI Concussion Database System web application to affiliated CCMI clinics, community care access centres, hospitals or other health care providers for the primary purpose of capturing and tracking information on patient concussion recovery, treatment, assessments, test results, and history. Health information custodians ("**HICs**") are required to sign a services agreement prior to being authorized to use the CCMI Concussion Database System. This electronic medical record (EMR) system, is used by partnered CCMI clinics and clinicians to record and track patient-related data.

CCMI Concussion Tracker Smartphone Application

CCMI provides the Concussion Tracker smartphone application to both patients/athletes and team leaders for the purposes of communication of injury status, return-to-school/work progressions, as well as return-to-play status. This information is only provided to individuals to whom the patient has consented to share this information with. Consent can be withdrawn at any time. The health information provided to team leaders includes pass or fail information relative to an athlete's baseline score during sideline testing and injury reporting as well as information concerning the recovery stage and current injury status of athletes/patients under their team list (contingent upon consent from the athlete/patient). Team leaders and patients are required to accept a Privacy Statement & Terms of Use, respectively, prior to being authorized to use the Concussion Tracker application.

CCMI Physician & Specialist Portal

CCMI provides access to patient concussion files through a multidisciplinary collaborative network via the CCMI Physician & Specialist Portal (the Portal). These are not CCMI partnered clinics but rather an access portal that a patient's family physician, sports medicine physician, or other medical specialist may access, from time to time, to check in on their patient. Users of this portal can view and add notes on a patient's file but they are not the main custodian of that file. The portal provides access to family physicians and various other specialists and healthcare professionals so that they may contribute to the multidisciplinary care of the patient. Access to a patient file is only provided via the patient's Concussion ID card as well as a 2-factor authentication process. All HIC's on the physician and specialist portal are required to agree to the CCMI HINP Privacy Policy as well as the terms of service agreement.