

CCIS Privacy Policy

Introduction

Hamilton Health Sciences (HHS) has been prescribed by the Regulation made under the *Personal Health Information Protection Act, 2004* (PHIPA) as a person responsible for maintaining Ontario's Critical Care Information System (CCIS) for the purpose of facilitating and improving health care (referred to as a "prescribed health registry"). PHIPA requires prescribed health registries to have privacy policies and related procedures in place, approved by the Information and Privacy Commissioner, to protect the privacy of the patients whose personal health information they receive and to maintain the confidentiality of the information.

This Privacy Policy demonstrates HHS's commitment to protecting personal health information according to PHIPA and the ten privacy principles found in the Canadian Standards Association (CSA) *Model Code for the Protection of Personal Information*.

Background

On January 30, 2006, the Ontario Ministry of Health and Long-Term Care (MOHLTC) announced a \$90 million Critical Care Strategy to ensure Ontario remains a global leader in providing critical care services and to improve access, quality and system integration in health care. The strategy identified seven components as priorities for provincial investment, including: (1) establishing Critical Care Response Teams to improve patient safety; (2) enhancing the skills of existing health care providers; (3) establishing a new Critical Care Information System (CCIS) to provide key data; (4) working together to improve performance and quality; (5) exploring ethical and legal issues with stakeholders; and (6) training more critical care physicians and nurses. One of the essential components of the strategy was the development of the provincial CCIS to collect and report on data supporting the information needs of the entire strategy.

The CCIS is a health registry that contains critical care data collected from hospital intensive care units (ICUs) across Ontario through a web-portal that, in turn, generates aggregate statistical reports on critical care metrics (i.e. bed availability, Admission/Discharge/Transfer (ADT) data and Critical Care Response Team (CCRT) activity) in order to facilitate resource allocation and bed management decision-making.

University Health Network (UHN) was appointed by the MOHLTC to manage the CCIS development and implementation across the province. UHN is also responsible for hosting the CCIS application at its secure data centre. As part of this responsibility, UHN has undertaken a Privacy Impact Assessment (PIA) to identify and mitigate against any potential privacy risks associated with the provincial roll out of the CCIS until the CCIS is formally transitioned to HHS, one of which was the need to develop CCIS specific information practices and procedures.¹ Once fully implemented, the business operations of the CCIS will be transitioned from UHN to HHS

¹ All privacy risks noted in the CCIS PIA have been addressed to date. A summary of the CCIS PIA has been provided to participating hospitals and can be requested from CCISFeedback@uhn.on.ca.

where the CritiCall Program (CritiCall) at HHS will be ultimately responsible for all CCIS information handling practices.²

Privacy Statements

1.1 Principle 1 - Accountability

An organization is responsible for personal health information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

The chain of accountability for personal health information collected, used, disclosed, and stored via the CCIS extends to HHS, as a prescribed health registry under the PHIPA regulation, UHN, the interim operator and manager of, and hosting service provider for, the CCIS, as well as CritiCall, the designated program area that manages the daily operations of the CCIS on behalf of HHS. The full commitment of HHS and UHN to PHIPA is required to ensure the confidentiality of CCIS data and that patient privacy rights are being respected.

To this end, HHS has designated a Chief Privacy Officer (CPO) who is accountable for ensuring overall compliance with PHIPA, this Privacy Policy and the privacy responsibilities described in the CCIS CPO Terms of Reference.³ The CPO, jointly with the CCIS Privacy Lead at UHN, is also responsible for overseeing the privacy component of the CCIS transition from UHN to HHS which involves providing privacy status updates and reporting any privacy and security issues to the CCIS Advisory Committee, the formal committee that was convened to oversee the CCIS strategy, implementation and operations.

The CPO at HHS is also accountable for developing and implementing staff training in relation to its CCIS. Staff privacy training must be provided to all CCIS end users at CritiCall and the members of the CCIS Provincial Project Team members at UHN to remind these individuals of their continuing privacy responsibilities for personal health information contained in the CCIS. The CPO must provide a CCIS privacy orientation session to new staff and ensure that refresher privacy training sessions are provided on an annual basis.

HHS and UHN are governed by a memorandum of understanding (MOU) which requires UHN to ensure the security of personal health information stored in the CCIS at all times and until the CCIS is transitioned to HHS. All participating CCIS hospitals must comply with the privacy obligations referenced in the Participation Agreement they signed (attached to the CCIS Critical Care Solution Master Service Level Agreement (MSLA) as a privacy schedule) that grants licensing terms for all CCIS users and requires CCIS data to be kept confidential and secure in accordance with PHIPA.

HHS relies on the IT department at UHN to provide information technology (IT) services such as servers, a data centre, computer support, and disaster recovery for the CCIS. The UHN IT

² CritiCall is a 24-hour-a-day provincial emergency referral program based out of HHS that links physicians throughout Ontario with on-call specialists, appropriate hospital beds, and assists in accessing appropriate transportation for critically ill patients.

³ The CCIS CPO Terms of Reference can be obtained by contacting CCISFeedback@uhn.on.ca.

Director is responsible for ensuring personal health information managed via these services is secure and managed in compliance with UHN's IT security policies. The Systems Security Specialist at UHN is responsible for day-to-day operation of IT security processes in respect of the CCIS. Security and production testing has been conducted on the CCIS and will be repeated, only as necessary, on an annual basis whenever major production releases are scheduled that may change the security configurations of the system.

Finally, this Policy and its supporting procedures are reviewed periodically **and when changes are made to legislation that governs HHS** to ensure that it continues to adhere to current legislative requirements and privacy best practices. The policy review is conducted by the CPO at HHS and/or his/her delegate(s). Any amendments to this policy must be approved by the CPO who in turn, must communicate these amendments to CritiCall staff⁴ and to the members of the CCIS Provincial Project Team at UHN, until the CCIS is transitioned to HHS.

This Policy will continue to apply to UHN until the CCIS is formally transitioned to CritiCall at HHS.

1.2 Identifying Purposes

The purposes for which personal health information is collected shall be identified by the organization at or before the time the information is collected.

The CCIS collects personal health information (i.e. critical care data) for the purpose of supporting the generation of statistical reports to facilitate decision-making related to resource allocation and bed management for the benefit of health care institutions across Ontario. The collection of patient-specific health information is required to enable several decision support benefits, such as assessing the effectiveness, efficacy and utilization of interventions on health outcomes for patients or assisting with individualized patient triage, transfer and discharge planning, among others. These benefits are communicated to all CCIS end users through the CCIS Data Collection Policy Guide and related CCIS Instructional Guide distributed to participating CCIS hospitals upon implementation.

In addition, patient specific demographic information is collected from each hospital system and displayed to CCIS data entry users to ensure that the correct patient is selected when admitting a critical care patient into the system and when updating patient life support interventions or CCRT assessments. Given that the CCIS has been designed to integrate with the EMPI in the future to track a patient's access to care across institutions and over time, details of a patient's full name, address, and health care number are required to uniquely identify the patient in accordance with the EMPI's specifications.

The purposes for which HHS collects personal health information via the CCIS health registry is reinforced to staff at CritiCall and the CCIS provincial team at UHN during privacy staff training sessions provided by the CPO at HHS.

1.3 Consent

⁴ For the purposes of this Policy, CritiCall staff means all employees, students, contractors or third parties who are employed or affiliated with HHS/CritiCall to support the CCIS operations.

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal health information, except where inappropriate.

HHS collects personal health information via the CCIS pursuant to its statutory authority under section 39(4) which permits prescribed health registries to collect personal health information without patient consent for the purpose of section 39(1)(c) (i.e. to improve or facilitate health care). PHIPA also permits other health information custodians, such as the Ministry's Enterprise Master Person Index (EMPI), and Cancer Care Ontario's Wait Time Information System (WTIS) to disclose personal health information to HHS without patient consent, as per section 39(1)(c) and 18(4), respectively. Given that all data flows via the CCIS are allowed to occur without patient consent, patients do not have the right to "lock" or opt out of providing their personal health information to hospitals for CCIS purposes. Such disclosures are expressly authorized under PHIPA.

During the CCIS implementation, HHS can rely on section 49(1) of PHIPA to disclose personal health information without patient consent to UHN in the interim, as the designated data steward to maintain the CCIS on its behalf. HHS can rely on its legal authority under section 49(1) to provide personal health information to CritiCall for the same purpose the information was collected in the CCIS, namely for section 39 health registry functions.

1.4 Limiting Collection

The collection of personal health information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

HHS ensures that the CCIS only collects the minimum data required (referred to as the "Provincial Core Data Set) to fulfill its mandate of supporting the generation of statistical reports to facilitate decision-making related to resource allocation and bed management for the benefit of health care institutions across Ontario. Specifically, the CCIS collects real-time data on inpatients (who may become ICU or CCRT patients) automatically from hospital ADT systems, while some hospitals enter this data manually. The CCIS is not a free-text system; radio buttons and drop down selections exist to limit the amount of data collected, which is comprised of the following information:

- **Patient demographics:** full name, date of birth, gender, health card number (e.g. Ontario Health Insurance Plan (OHIP) number), medical record number (MRN), full address, phone number;
- **Patient data:** ICU admission source/service/time/date, admitting diagnosis, discharge destination;
- **CCRT status:** time and date CCRT notified, ICU admission time (if applicable), time and date seen by CCRT, occurrence of end-of-life discussion with patient, among other data elements;
- **Bed availability:** total number of beds (i.e. number of open, closed or beds with ventilator capacity); and
- **Life support interventions:** ventilator status, CVL or Arterial Line status, vasoactive/inotropic meds, ICP monitor and continuous dialysis status.

The Provincial Core Data Set was vetted by an advisory group comprised of intensivists, critical care researchers and other key health stakeholders to determine the required CCIS data elements which were based on patient safety concerns, improved resource access considerations and service uptake factors.

1.5 Limiting Use, Disclosure and Retention

Personal health information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Personal health information contained in the CCIS will only be used, disclosed, and retained for the purpose for which it was collected.

Limiting Use

The CCIS utilizes role-based access controls to restrict the types of information that may be used to a “need-to-know basis” in order for CriteCall staff and the CCIS provincial team to perform their duties in relation to the CCIS. Furthermore, the ICU discharged patient list is only accessible to CCIS end users for 7 days.

Limiting Disclosure

The CCIS discloses reports mostly in the form of aggregate statistics and trended indicators for critical care planning purposes. Patient specific information (available in the form of the CCIS portal's Active Patient List or Core Data Export) is disclosed only to authorized personnel at hospitals (e.g. ICU unit clerks, nurse managers, nurses, data analysts, hospital executives and CCRT coordinators) for the following purposes:

- assisting hospitals in locating critical care resources for a patient who is critically ill, either in their own hospital or within the LHIN;
- quickly identifying the patients who are in the ICU, by diagnosis and life support interventions, and therefore supporting ICU staffing and technology decisions; and
- linking ICU patient data with Critical Care Response Team (CCRT) patient data so that care outcomes can be compared.

Before downloading any identifying patient data as part of a Core Data Export, users will be able to filter the report by date, entity (hospital, site or unit within that hospital), and choose whether or not they would like to include personal health information.

Limiting Retention

The CCIS is designed to retain personal health information only as long as necessary to fulfill the purpose for which it was collected and in the least identifiable form possible (for example, patient names and other identifiers can be removed once they are no longer required). All inpatient information received from hospital ADT systems is retained for seven days post discharge from the hospital ADT. The CCIS retains ADT information for one year on patients who have not been discharged from the ADT system. Critical care reports generated by the CCIS in de-identified, aggregate format is retained indefinitely for historical analysis purposes.

CritiCall staff is responsible for the confidential destruction of CCIS data printed from the CCIS when it is no longer required to support a function of the CCIS. CritiCall staff is also responsible for physically destroying CCIS data retained outside the system in soft-copy (e.g. compact disk) to the point that it cannot be reconstructed or sending the portable media to the CPO at HHS, who is responsible for disposing of it in accordance with HHS's media disposal policies.⁵

These retention and disposal requirements apply equally to the CCIS provincial team at UHN who have access to CCIS data for technical support and other legitimate CCIS purposes.

1.6 Accuracy

Personal health information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

The quality and completeness of individual identifying information that is collected via the CCIS from hospital ADT systems determines the integrity of the CCIS data and in turn, the accuracy of the statistical reports generated via the CCIS. Accordingly, the primary responsibility for ensuring that personal health information accessed via the CCIS application is as accurate, complete, and up-to-date as is necessary for the purposes for which it was collected (to facilitate and improve the delivery of care) falls to individual CCIS users (e.g. intensive care unit nurses, clerks, CCRTs, clinicians, including support staff at hospitals). Hospitals using the CCIS application are also responsible for notifying recipients of any limitations, of which they are aware, to the accuracy, completeness, or up-to-date character of the information. This responsibility is outlined in the privacy schedule attached to the MSLA entered into between Navantis Inc., the CCIS application service provider, UHN and all participating CCIS hospitals.

The CCIS reports are designed to reflect a near "real-time" view of ICU resource utilization. Specifically, ICU data is updated twice daily in two 12 hour time blocks and automated report generation is done twice daily to reflect that data.

1.7 Safeguarding Data

Personal health information shall be protected by security safeguards appropriate to the sensitivity of the information

CritiCall at HHS and the members of the CCIS Provincial Project Team at UHN employ administrative, technical, and physical safeguards to protect personal health information in their custody and control against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. These safeguards apply to personal health information in paper or electronic form and while in storage or in transit.

Administrative Safeguards

Administrative safeguards have been implemented through contractual means, such as the MSLA applicable to Navantis, UHN and all participating hospitals. The MSLA includes a privacy schedule containing specific privacy protective clauses to prevent unauthorized access to and

⁵ HHS Media Disposal Policy: *HIS -Destruction of Personal Health Information.*

disclosure of personal health information, with notification requirements for hospitals for privacy breaches, among other things.

The MOU between HHS and UHN identifies the security safeguards in relation to the hosting and network services to be provided by UHN for the CCIS. This agreement outlines the specific permitted uses by UHN on behalf of HHS and includes restrictions for access by employees and contractors of UHN while the CCIS is in its custody and control, among other things, such as the requirement to securely return or destroy personal health information once the CCIS is transitioned from UHN to HHS.

The CPO is responsible for ensuring all CritiCall staff have undergone training on this Policy and have confirmed their understanding of this Policy by signing a CCIS Confidentiality Agreement. The CPO must ensure that a CCIS confidentiality agreement is signed when new staff begins his or her employment with HHS. The Privacy Lead at UHN must also ensure that similar confidentiality obligations for the CCIS provincial team are followed by having staff sign the CCIS Confidentiality Agreement and ensuring all access rights to the CCIS are extinguished when the CCIS is transitioned to CritiCall at HHS.

Technical safeguards

The CCIS application is built with single sign-on, role-based access and password controls so that only authorized hospital CCIS users may access the CCIS. All CCIS data transmissions are encrypted using a Secure Socket Layer (SSL). UHN provides a secure virtual private network (VPN) connection to protect CCIS data from unauthorized access. The CCIS also provides complete audit capability for usage, including login, logout, functional areas visited and major operations performed. The audit log tracks every screen a user viewed, by patient, irrespective of whether any modification occurred. The content of the log will include information such as which end user is accessing which patient information and the time when the information is accessed. If a user modifies data, the detail of those changes will also be logged.

As noted above, reports that include patient-specific information are available only to authorized personnel and in accordance with each hospital's own policies and procedures regarding access to patient information. The CCIS is designed with role-based access controls so that only authorized users can access patient health and demographic information. For example, hospital employees only have access to the clinical information of patients registered as patients at that facility.

The CCIS Provincial Project Team has conducted a Network and Application Security Audit as well as a Security Penetration Test to assess the security of the CCIS application and its supporting infrastructure which included the following:

- ✓ **Network Assessment** – to evaluate security controls in place at the network layer, including overall design, firewalls, routers, switching, virtual private networking and intrusion detection;
- ✓ **Host Assessment** – to evaluate a sample of ten host servers (operating system, middleware, LDAP/Active Directory and Internet services used to deliver the application. Security configuration of CCIS was compared to best practice standards, such as NIST, Cert, NSA, and others;

- ✓ **Database Assessment** – to evaluate configuration, access controls, auditing and security over data storage (date encryption) and compare to best practice standards. Controls were evaluated for known threats such as SQL injection, vendor based vulnerability, etc.
- ✓ **Application Assessment** – to assess the functions and platform of the application from both a client and server perspective and evaluate controls around authentication and user access, segregation of duties, business logic and transaction process, etc.; and
- ✓ **System Application Penetration Test** – to test the remote application via the VPN in order to access and penetrate the CCIS internal network.

Physical Safeguards

The CCIS is physically stored by UHN at a secure Data Centre in Ontario. Therefore, UHN is responsible for the physical security of the CCIS. The Data Centre has a security portfolio that strengthens application-level security with advanced identity provisioning and physical access controls, including restricted access to its operational environment and video monitoring. Furthermore, the Data Centre has resilient power, Heating Ventilation Air Conditioning (HVAC), and fire controls that are optimally clustered, to ensure that no data will be lost if a server goes down. These physical safeguards are supported by strict access policies and procedures.

1.8 Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal health information.

HHS makes information about its privacy practices and the collection, use, and disclosure of personal health information via the CCIS available to CritiCall staff, the general public, and participating hospitals. This information is available upon request to the CPO and at the Ministry's website:

http://www.health.gov.on.ca/english/providers/program/critical_care/cct_infosystem.html

In addition, the CPO at HHS ensures that the following information is readily available:

- general information on CCIS information handling practices;
- a descriptions of data the CCIS collects and retains; and
- contact information on how to contact the CPO.

The CCIS provincial team at UHN also provides CCIS materials to participating CCIS hospitals to assist them in answering questions from patients and their families about the CCIS. CCIS Frequently Asked Questions and Answers (FAQs) can be obtained by contacting CCISFeedback@uhn.on.ca. These FAQs have also been provided to the CCIS project manager at each participating hospital.

All CritiCall staff immediately direct enquires for information about CCIS privacy practices to the CPO. During site implementation, there are CCIS Provincial Team site coordinators for each participating hospital to answer any privacy-related CCIS questions. Finally, the Privacy Lead at UHN is also responsible for responding to CCIS questions or concerns and will work in collaboration with the CPO at HHS in resolving any privacy related issues.

1.9 Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal health information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Patients wishing to access their records of personal health information, or to request amendments to records of personal health information, in the CCIS will be instructed to contact the CPO at CritiCall/HHS, who in turn will refer the patient to the physician who, or hospital that, originally entered their personal health information into the CCIS. These physicians or hospitals are responsible for providing patients with access and implementing corrections to their records.

1.10 Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Individuals can submit their privacy concerns or complaints regarding the CCIS to the CPO at CritiCall/HHS at CCISFeedback@uhn.on.ca or in writing to Chief Privacy Officer, Hamilton Health Sciences, Chedoke Site, Ewart Building, Room 311, 559 Sanatorium Rd., Hamilton, Ontario, L9C 7W8.

The CPO reviews all privacy concerns and complaints related to CCIS. If a complaint is found to be justified, the CPO will conduct an investigation and take appropriate measures including, if necessary, amending its policies and procedures.

Individuals may also make a complaint to the Information and Privacy Commissioner/Ontario.

Privacy or security questions or concerns relating to the CCIS, including any questions regarding CCIS-specific privacy and security policies can also be directed to each participating hospital's CCIS Provincial Team site coordinator or to the Privacy Lead for the CCIS provincial team at UHN: CCISFeedback@uhn.on.ca.

References:

- Ontario *Personal Health Information Protection Act, 2004*.
- Canadian Standards Association's *Model Code for the Protection of Personal Information*.
- Letter from the Information and Privacy Commissioner/Ontario to CritiCall Ontario, July 11, 2007.
- Letter to the Information and Privacy Commissioner/Ontario from CritiCall Ontario, September 14, 2007.
- CCIS Privacy Impact Assessment.

The following related must be followed in conjunction with this CCIS Privacy Policy:



Part of the Province's Critical Care Strategy

- CCIS Chief Privacy Officer – Terms of Reference, November 21, 2007.
- CCIS Access Control Procedure, November 21, 2007.
- CCIS Privacy Breach Management Procedure, November 21, 2007.
- CCIS Privacy Training and Awareness Session (PowerPoint slides).
- HHS Media Destruction Policy and Procedure: *HIS -Destruction of Personal Health Information.*
- CCIS Confidentiality Agreement (to be signed by CCIS users at CritiCall).

Effective Date:	November 21, 2007
Last Revised:	
Approved By:	