Critical Care Information System (CCIS) Frequently Asked Questions (FAQ's)

Background

On January 30, 2006, the Ontario Ministry of Health (MOH) 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 healthcare.

The strategy identified seven components as priorities for provincial investment, including: (1) establishing Critical Care Response Teams ("CCRT"s) 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.

Below are some ***Frequently Asked Questions*** about the privacy and security of the CCIS.

What is the CCIS (Critical Care Information System)?

The CCIS is a health registry that contains critical care data collected from hospital critical care units across Ontario. The data is entered by CCIS trained and authorized critical care unit staff through a secure web-portal that generates aggregate statistical reports on critical care services (i.e. bed availability, Admission/Discharge/Transfer (ADT) data and CCRT activity). This data is used to facilitate resource allocation and bed management decision-making.

What is the Status of the CCIS under the *Personal Health Information Protection Act* (PHIPA)?

Hamilton Health Sciences (HHS) has been prescribed by the Regulation (329/04, Section 13 (1)(5) that accompanies PHIPA as a person responsible for maintaining the CCIS for the purpose of facilitating and improving the provision of health care. HHS has delegated the day-to-day operation and management of the CCIS to CritiCall Ontario (CritiCall), a provincial program administered by HHS and funded by the MOH.

What are HHS/CritiCall's Responsibilities under PHIPA?

PHIPA requires prescribed persons to have privacy policies and related procedures in place and approved by the Information and Privacy Commissioner of Ontario (IPC) every 3 years, to protect the privacy and confidentiality of the personal health information (PHI) within the CCIS.

PHI is defined in PHIPA as:

"Identifying information" about an individual, whether oral or recorded if the information:

- relates to the individual's physical or mental condition, including family medical history,

- relates to the provision of health care to the individual,
- is a plan of service for the individual,
- relates to payments, or eligibility for health care or for coverage for health care,
- relates to the donation of any body part or bodily substance or is derived from the testing or examination of any such body part or bodily substance,
- is the individual’s health number or
- identifies a health care provider or a substitute decision-maker for the individual.

The Chief Executive Officer (CEO) of HHS is ultimately accountable for the protection of PHI in the custody or control of the CCIS. The CEO has delegated the day-to-day responsibility for overseeing the CCIS to the CritiCall Executive Director. The Executive Director is responsible for overseeing compliance with PHIPA, CCIS privacy and security policies, and CCIS procedures and practices.

The Executive Director, has appointed a CritiCall Privacy Manager who is responsible for the day-to-day privacy operations, compliance and management. The Executive Director has also appointed a Manager of IT, Applications & Security Lead works closely with the Privacy Manager and oversees complementary security operations and management.

CritiCall staff members are employees of HHS and as such, upon hire, sign confidentiality agreements. New employees are provided with initial corporate privacy and security training. Additionally, all CritiCall staff members undergo CritiCall specific annual privacy and security training.

Staff members with job-related duties specific to the CCIS undergo additional role-based privacy and security training. They must also sign and annually renew confidentiality agreements specific to their obligations related to the CCIS.

CritiCall makes privacy and security policies and procedures available electronically to all Ontario hospitals participating in the CCIS as well as to vendors and any other agents that support the CCIS. Through contracts and agreements, CritiCall further requires vendors and other agents that support the CCIS to acknowledge and agree to their obligations to protect and keep confidential the PHI within the CCIS.

Hospitals that participate in the CCIS enter into data sharing agreements with HHS. Hospitals are responsible for the PHI that they collect and enter into the CCIS while HHS/CritiCall is responsible for the PHI once received.

What PHI is collected by the CCIS?

The CCIS collects a number of data elements about critical care patients, the hospitals and units where they are receiving care, and the types of care required during the course of their stay in the critical care unit.

PHI collected in the CCIS include the following data elements:

- Patient name
- Medical record number
- Date of birth
- Age
- Gender
- Health card number and type

All data are entered by CCIS trained and authorized hospital staff working in critical care units of Ontario hospitals. Each of these hospitals has entered into data sharing agreements for the CCIS.

Intensive Care Unit (ICU) /Critical Care Unit (CCU) staff members receive CCIS training and have electronic access to all CCIS policies and procedures, including those related to privacy and security, through the CCIS Document Library.

How is the CCIS data used?

The CCIS has been developed to provide real time data on every patient admitted to Level 3 and Level 2 Critical Care Units in Ontario's acute care hospitals. It is intended to provide the MOH, Local Health Integration Networks (LHINs)/Regions and hospital leaders with information such as bed availability, critical care services utilization and patient outcomes.

The CCIS also supports performance measurement which is intended to facilitate decision making and highlight opportunities for implementing quality improvement initiatives. This is done through the collection of data, entered in real time for every critically ill patient admitted to a CCU. The core data export functionality allows end-users to download their own hospital data from the CCIS for additional analysis. CCIS users can also access a variety of system-generated reports through the CCIS.

CCIS data is also used by CCSO to generate Quarterly/scorecard reports for specific indicator, which is distributed to various provincial stakeholders. These reports enable evidenced-based decision making, support system-wide planning, and informs potential capital investments.

PHI collected for the CCIS is limited to that which is necessary to fulfill the above purposes. Please refer to *'P5-List of Data Holdings and P7-Statements of Purpose for Data Holdings Containing Personal Health Information'* for a list of the data elements contained within the CCIS.

Is CCIS data disclosed?

In addition to disclosing aggregate data to Critical Care Services Ontario (CCSO) as a PHIPA Agent of HHS/CritiCall (with respect to CCSO's role in strategic oversight of the CCIS), CritiCall provides data back to individual hospitals that participate in the CCIS.

CritiCall also accepts and reviews requests for CCIS data for research and non-research purposes, via applications submitted to CritiCall (forms available on the website), where the requestor may be authorized to receive CCIS data.

All research requests must have prior approval from a researcher's Research Ethics Board before being submitted. All other requests are reviewed on a case-by-case basis and are based on the authorities provided by PHIPA, including authorization to disclose (i.e. to a prescribed entity). Once submitted, the requests are reviewed by the CritiCall Privacy Manager and subsequently the CCIS Data Stewardship Committee to make a formal determination around disclosure. If approved, requestors/researchers must enter into a data sharing agreement with HHS/CritiCall that requires them to ensure the protection of the PHI throughout the course of study, and its secure destruction after study completion.

Patients may also request access or corrections to their own CCIS data by contacting the CritiCall Privacy Manager or the hospital that originally entered their PHI into the CCIS. These hospitals are responsible for processing patient access and correction requests and will liaise with CritiCall as required.

As HHS is also an 'institution' under the *Freedom of Information and Protection of Privacy Act* (FIPPA), Access requests can also be made for Personal Information (PI) under FIPPA. In these cases, CritiCall will transfer the request to the hospital that has collected the PI.

How does HHS/CritiCall ensure the protection of the PHI within the CCIS?

HHS/CritiCall has implemented administrative, physical and technical safeguards to help ensure the protection of the PHI within the CCIS. These are detailed in CCIS policies and procedures that are available through the CCIS Document Library or upon request to the CritiCall Privacy Manager.

Some of the safeguards are outlined below:

Administrative Safeguards:

- More than 35 policies and procedures documenting requirements and procedures related to privacy, security, human resources and organizational expectations pertaining to the CCIS
- More than 15 Logs documenting adherence to policies and procedures
- Committee structures to support operational and research aspects of the CCIS
- Privacy Impact Assessments
- Threat Risk Assessments
- Ongoing privacy and security training and awareness for staff
- Confidentiality and contractual agreements

Technical Safeguards:

- Our cloud vendor provides services that help us protect our data, accounts, and workloads from unauthorized access, data protection services that provide encryption capabilities, key management, and sensitive data discovery to help us protect our data and workloads.
- Our Cloud Vendor environments are continuously audited, with certifications from accreditation bodies.

- End to End Encryption of all CCIS data in transit and at rest.
- Secure portal access to CCIS for user authentication.

Physical Safeguards in Cloud:

- Our Cloud Vendor controls provide reasonable assurance that data centers are protected against unauthorized physical access and environmental threats.
- Audit information is provided on a regular basis per vendor agreements and schedules, satisfying legal frameworks such as PHIPA and regulatory frameworks such as IPC audits.

What steps does CritiCall take in relation to CCIS to protect PHI from theft, loss and unauthorized use, disclosure or unauthorized copying, modification or disposal?

Access to the CCIS is provided on a "need-to-know basis" and restricted only to employees, vendors and other agents that require access to perform job-related functions. Access is also role-based to ensure those being granted have access only to the information they require for the purposes of their role. Access to the CCIS is audited to ensure information is being accessed appropriately and for the purposes for which it is required.

CCIS data is housed in cloud with Physical Security and Environmental Protection controls which provides reasonable assurance that Data Centers are protected against unauthorized physical access and environmental threats. All safeguards are taken in compliance with relevant regulatory frameworks and legal obligations, such as the Patient Health Information Protection Act.

All staff, contractors and other agents receive privacy and security training and education and are bound by contractual agreements (i.e. confidentiality agreements or contract clauses related to privacy and security requirements) to protect the PHI in the CCIS. All data actions including disclosure and destruction are governed by a combination of the aforementioned contracts and regulatory frameworks as established by relevant bodies, such as the Integrity & Privacy Commissioner of Ontario.

A Breach Management Policy and Procedure is in place for both privacy and security incidents to ensure that incidents, or incidents determined to be security and/or privacy breaches are appropriately contained, documented, investigated, and remediated.

How can I find out more information or make an inquiry or complaint?

Please contact the CritiCall Privacy Manager for all inquiries, complaints or information requests related to the CCIS.

Contact information for the CritiCall Privacy
Manager is below:
Email: privacy@criticall.org

Post:
Attention CritiCall Privacy Manager
1725 Upper James Street

Suite 200
L9B 1K7

By Telephone:
(905) 308-3681

Individuals may also make a complaint to the Information and Privacy Commissioner of Ontario. The Information and Privacy Commissioner/Ontario may be contacted:

By Email:
info@ipc.on.ca

Post:
Information and Privacy Commissioner of Ontario
2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

By Telephone:
(416) 326-3333