Hamilton Health Sciences	**Critical Care Information System –Privacy**
Title: P1 - Privacy Policy in Respect of HHS as a Prescribed Person	
Posting Date: July 7, 2014	
Approved By: MaryWall, Director Privacy and Freedom of Information (FOI), HHS; Mark Farrow, Chief Security Officer, HHS; Donna Thomson, Executive Director, CritiCall Ontario	
Date of Initial Approval: June 24, 2014	**Date of Last Review:** September 30, 2016
Date of Next Review: June 2017	

Version History			
Version No.	**Date**	**Summary of Change**	**Changed By**
1.1	July 10, 2015	Refined privacy training statement Clarified where FAQs are available	Christine Moon, CritiCall Privacy Lead
1.2	May 10, 2016	No major changes Simplified "Applies to" language	
1.2	Sept 30, 2016	Revised Privacy Committee responsibilities and reporting requirements of CritiCall privacy Lead	Mary Wall, Director Privacy and FOI, HHS

Applies To:

This policy applies to all Hamilton Health Sciences (HHS)/CritiCall Ontario (CritiCall) employees any other agents of HHS/CritiCall[1]and hospitals that support the ongoing operation, management and maintenance of the Critical Care information System (CCIS).

[1]Agents may be employees, consultants, contracted workers, vendors or any other person who acts on behalf of HHS/CritiCall in respect of personal health information for the purposes of HHS/CritiCall and not the agent's own purposes, whether or not the agent has the authority to bind HHS/CritiCall and whether or not the agent is employed by the HHS/CritiCall and whether or not the agent is being remunerated.

Purpose

The purpose of this policy is to outline the privacy practices for HHS as a Prescribed Person in respect of the CCIS under the *Personal Health Information Protection Act*, 2004 (PHIPA) as it relates to the collection, use and disclosure of personal health information (PHI).

Background

On January 30, 2006, the Ontario Ministry of Health and Long-Term Care 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.

The CCIS is a health registry that contains critical care data collected from hospital critical care units across Ontario through a web-portal that, in turn, generates aggregate statistical reports on critical care services (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)/Critical Care Services Ontario (CCSO) was appointed by the Ministry of Health and Long-Term Care (MOHLTC) to develop the overall strategy for the CCIS. The MOHLTC has assigned responsibility for the management and day-to-day operations of the CCIS to Hamilton Health Sciences Corporation (HHS). HHS operates the CCIS as a part of its CritiCall Ontario Program (CritiCall). HHS is ultimately responsible for all CCIS information handling practices.

Status Under the Act

HHS has been prescribed by the Regulation[2]that accompanies PHIPA as a person responsible for maintaining the CCIS for the purpose of facilitating and improving the provision of health care. PHIPA requires prescribed persons, who compile a health registry, to have privacy policies and related procedures in place and approved by the Information and Privacy Commissioner/Ontario (IPC/O) every 3 years, to protect the privacy and confidentiality of the PHI within the CCIS.

This Privacy Policy demonstrates HHS's commitment, as a prescribed person, to protecting PHI according to PHIPA, its Regulation and the ten privacy principles found in the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information.

[2]*Ontario Regulation 329/04*, Section 13(1)(5).

Policy Statement
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 Chief Executive Officer (CEO) at HHS is ultimately accountable for ensuring CCIS compliance with the PHIPA, CCIS privacy and security policies, procedures, practices and all CCIS obligations as a prescribed person. The CEO at HHS has delegated oversight for ensuring overall compliance with PHIPA, its regulation and this Privacy Policy to the Director of Privacy and Freedom of Information. The HHS Director of Privacy and Freedom of Information, jointly with the Executive Director at CritiCall, are delegated by the CEO of HHS to oversee compliance with the Act and its regulation, and for ensuring compliance with the CCIS privacy and security policies, procedures and practices.

The Executive Director at CritiCall has appointed a CritiCall Privacy Lead who is responsible for the day-to-day privacy operations, compliance and management. The CritiCall Privacy Lead is responsible for all activities identified within the job description for the CritiCall Privacy Lead, including a) privacy training for all employees and agents assigned to the CCIS project, b) privacy breach management and c) privacy risk management activities. The CritiCall Privacy Lead reports directly to the Executive Director at CritiCall.

The CritiCall Information Technology department oversees and manages the CCIS hardware and services. The Executive Director, CritiCall has delegated responsibilities for ensuring PHI managed via these services is secure and maintained in compliance with the CCIS Security policies, such as security training, security reviews, security incident resolution, physical security of the CritiCall premises to the CritiCall Security Lead. The CritiCall Security Lead and the CritiCall Privacy Lead, both report directly to the Executive Director, CritiCall and together shall resolve any security issues that may impact PHI in CCIS.

The CCIS Data Stewardship Committee is a formal committee convened to oversee the CCIS data holding. This committee is co-chaired by the CritiCall Executive Director and a representative from CCSO and includes members from HHS/CritiCall, CCSO and relevant stakeholders. This committee receives reporting on all issues that impact the CCIS data holding and requests for CCIS data. This Committee reports to the CritiCall Executive Council.

The CritiCall Privacy Lead shall complete a quarterly report on privacy and security and provide the report to the CritiCall Executive Council for review. The CritiCall Privacy Lead shall also complete an annual report on privacy and security which is reviewed and approved by the Executive Vice President Clinical Operations and Chief Operating Officer.

Together, the CCIS Data Stewardship Committee as well as the Director, Privacy and FOI provide direction to the Executive Director, CritiCall and CritiCall Privacy Lead in respect of matters related to the protection of PHI and compliance with PHIPA.

This Policy and its supporting procedures are reviewed periodically and when changes are made to legislation that governs HHS in its role as a prescribed person. Updates to the policy will be made to ensure that it continues to adhere to legislative requirements and privacy best practices. The policy review is conducted by the CCIS Privacy Lead, Executive Director, CritiCall and the Director, Privacy and FOI and/or his/her delegate(s). Any amendments to this policy must be approved by the Executive Director, CritiCall and the Director Privacy and FOI, HHS.

Principle 2 - Identifying Purpose
The purposes for which personal health information is collected shall be identified by the organization at or before the time the information is collected.

HHS collects PHI (i.e. critical care data) from health information custodians 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. HHS does not collect any PHI directly from individuals.

The collection of patient-specific health information is required to create decision support tools for 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. The benefits and the purpose for collection are communicated to all CCIS end users through the CCIS Data Collection Guide and the CCIS Instructional Guide distributed to participating CCIS hospitals. Additionally, data sharing agreements between each hospital and HHS, with respect to the CCIS clearly outline the purpose of data collection.

The purposes for which HHS collects PHI is provided to HHS/CritiCall employees who have access to CCIS PHI (i.e. CCIS Educators, Information Technology and Decision Support staff) during privacy training sessions provided by the CritiCall Privacy Lead.

Principle 3 - Consent
The knowledge and consent of the individual are required for the collection, use, or disclosure of personal health information, except where inappropriate.

HHS collects PHI pursuant to its statutory authority under section 39(4) which permits prescribed persons to collect PHI without patient consent for the purpose of section 39(1)(c) (i.e. to improve or facilitate healthcare). Given that all collection of PHI by HHS occurs without patient consent, patients do not have the right to "lock" or opt out of HHS collecting their PHI from hospitals.

This CCIS Privacy Policy is publicly available, along with a description of the purposes for HHS's collection, use and disclosure of PHI. Health information custodians that disclose PHI to HHS are also required to have in place information practices describing the purposes for which they collect, use, disclose, retain and dispose of PHI, as well as the safeguards they use to protect PHI.

Principle 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 is committed to not collecting more PHI than is necessary to fulfill its mandate and will not collect PHI, if other information will serve the same purpose. Specifically, HHS collects real-time data automatically from integrated hospital admission discharge transfer (ADT) systems. Hospital systems which are not integrated with CCIS enter data manually to CCIS through an online portal. The information collected by hospitals is done via a 256 bit secure VPN connection over the eHealth network. 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 found in the CCIS data set:

Patient demographics: full name, date of birth, gender, full address, phone number;

Patient data: ICU admission source/service/time/date, admitting diagnosis, discharge destination; health card number (e.g. Ontario Health Insurance Plan (OHIP) number), medical record number (MRN);

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, PELOD, PIM2, MODs and continuous dialysis status.

The CCIS 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 based on patient safety concerns and improved resource access considerations. The Director, Privacy and FOI has reviewed the CCIS data set to ensure that it is consistent with the collection of PHI permitted by PHIPA and its regulation.

HHS is committed to only collecting that information which is necessary to fulfill its goal of providing aggregate reporting to support the Ontario Critical Care Strategy. In this regard, the *P4 -Policy and Procedure for the Collection of Personal Health Information*, has been developed and implemented to ensure the amount and type of PHI collected by HHS is limited to only that which is necessary to fulfill its mandate. The *P4 -Policy and Procedure for the Collection of Personal Health Information* outlines:

- The review and approval process for changes to the current CCIS PHI data set;
- Conditions for approval and any restrictions on data collection; and
- Secure Retention, Transfer and Return/Disposal of PHI.

A full listing of data holdings of PHI maintained by the HHS and the data elements/data sources for those data holdings is found in *P5 - List of Data Holdings Containing Personal Health Information* and *P7 - Statements of Purpose for Data Holdings Containing Personal Health Information.*

Principle 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.

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

Limiting Use

HHS, in its role as a prescribed person, uses the PHI collected from Ontario hospitals through the CCIS to create aggregate level reporting on bed availability, critical care service utilization and patient outcomes data. These aggregate level reports do not contain any PHI and are provided to the Ministry of Health and Long-Term Care, Local Health Integration Networks (LHINs) and hospitals to facilitate the allocation of resources and funds for improving critical care services in Ontario.

PHI contained in the CCIS will not be used internally by HHS or CritiCall for research purposes. A principal investigator conducting a research ethics board approved study may request PHI from the CCIS application. Release of PHI from the CCIS application to an approved research study is considered to be a disclosure of PHI and shall be considered and processed in compliance with s. 44 of PHIPA and the *P13 - Policy and Procedures for the Disclosure of PHI for Research Purposes and the Execution of Research Agreements*.

A robust set of policies, procedures and agreements has been developed and implemented to ensure that PHI collected and used by CCIS is done so in a manner consistent with PHIPA and its regulation. Furthermore, CCIS shall not use PHI if other information will serve the purpose, nor use more PHI than is reasonably necessary to meet the purpose for using the information.

As a prescribed person, HHS remains responsible for the PHI used by those with the authority to access CCIS and has developed polices, procedure and agreements to limit the collection, use, disclosure, retention and disposal of PHI including the following HHS policies in respect of CCIS:

- *P8 –Policy and Procedure for Limiting Agent Access to and Use of Personal Health Information;*
- *P10 –Policy and Procedure for the Use of Personal Health Information for Research;*
- *S14 –Policy and Procedure on the Acceptable Use of Technology; and*
- *P19 –Policy and Procedure for the Execution of Data Sharing Agreements.*

In addition to policies, procedures and agreements which limit the use of PHI, HHS utilizes role-based access controls to restrict the types of information that may be used to a "need-to-know basis" in order for HHS/CritiCall employees and others authorized to access CCIS to perform their duties in relation to the CCIS.

Limiting Disclosure

HHS discloses PHI:

a) To researchers for research studies. Research studies that have been approved by a Research Ethics Board may submit a request to HHS in respect of the CCIS, in writing, for access to PHI. Each submission from a research study must meet the requirements outlined in section 44 of PHIPA. Submitted studies are reviewed by the CCIS Data Stewardship Committee. If a study is approved by the CCIS Data Stewardship Committee, the researcher must enter into an agreement with HHS stipulating the terms for the use, disclosure, security, return, or disposal of the PHI disclosed by HHS from the CCIS; the *P13-Policy and Procedures for the Disclosure of Personal Health Information for Research Purposes and Execution of Research Agreements* governs all disclosures of CCIS data to a research study;
b) To another prescribed person or entity for purposes related to the duties of that prescribed person or entity, other than research; and
c) If required by law (i.e. pursuant to a request by law enforcement).

HHS discloses aggregate statistical reports and trended indicator reports for critical care planning purposes. Patient specific information is not included within these aggregate reports. Reporting is provided to the Ministry of Health and Long-Term Care, Local Health Integration Networks, Critical Care Services Ontario and hospitals. These reports provide vital decision making analysis used to improve resource allocations for critical care patients. All aggregate reporting is reviewed prior to its disclosure in order to ensure that there is no PHI included and to ensure that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. Data is aggregated or de-identified in accordance with the *P24 -CCIS Policy and Procedure with Respect to De-Identification and Aggregation.*

HHS ensures that any PHI it discloses is done in a manner consistent with PHIPA and its regulation. Furthermore, the HHS shall not disclose any PHI if other information will serve the purpose, nor disclose more PHI than is reasonably necessary to meet the purpose for the permitted disclosure. The following are some of the policies which govern the disclosure of PHI by the CCIS:

- *P12 – Policy and Procedure for Disclosure of Personal Health Information for Purposes other than Research;*
- *P24 - Policy and Procedure with Respect to De-Identification and Aggregation; and*
- *P13 – Policy and Procedure for Disclosures of Personal Health Information for Research and the Execution of Research Agreements.*

Limiting Retention

HHS only receives PHI in electronic format and retains that PHI only as long as necessary to fulfill the purpose for which it was collected and in the least identifiable form possible. Electronic data is transferred into the CCIS through a 256 bit secure VPN connection over the eHealth Ontario network in a secure manner in accordance with industry best practices.

The PHI received from hospitals is retained in an electronic format for up to one year within the CCIS and in accordance with the *S5 -Policy and Procedure for the Secure Retention of Records of Personal Health Information*. After one year, the PHI is purged from the CCIS by means of deletion of data stored within the integrations database and in compliance with the *S8-CCIS Policy and Procedure for the Secure Disposal of Records of Personal Health Information*. Additionally, any CCIS system equipment which is replaced or retired will be destroyed as per the *S8 -CCIS Policy and Procedure for the Secure Disposal of Records of Personal Health Information*.

Critical care aggregate reports generated by HHS/CritiCall are retained indefinitely for historical analysis purposes.

All HHS/CritiCall employees and agents that are assigned to support the CCIS are responsible for permanently destroying (e.g. through irreversible shredding) PHI printed from the health data registry once the information is no longer required. PHI in paper form shall be secured at all times, as stated within the *S3 -Policy and Procedure for Ensuring Physical Security of Personal Health Information*.

These retention and disposal requirements apply equally to all field and office employees and agents who support the CCIS prescribed person activities.

Principle 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 PHI that is collected via the CCIS from hospital 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 PHI 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 workers at hospitals). Hospitals using the CCIS application are responsible for ensuring the accuracy of the data entered into the CCIS. Changes may be made at the unit level as long as the patient is active within CCIS or for up to 72 hours following discharge. CLI, VAP and unplanned extubation data is publicly reported and hospitals are responsible for reviewing their own data for these indicators. For the highest data quality, the expectation is that VAP/CLI will be monitored daily by the most appropriate clinical and/or infection control staff and reported on as incidents are diagnosed. Incidents can be removed in the CCIS at any time during a patient's stay and up to 72 hours after

the patient is discharged from the critical care unit or until they are admitted to another critical care unit that is active in CCIS.

Principle 7 – Safeguarding Personal Health Information
Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

HHS, in respect of the CCIS, employs administrative, technical, and physical safeguards to protect PHI in its custody and control against loss or theft, as well as unauthorized access, disclosure, copying, use, disposal or modification. These safeguards apply to PHI in paper or electronic form.

Administrative Safeguards

Some of the administrative safeguards that have been implemented for the CCIS are:

- Contracts with vendors, employees, agents and all participating hospitals. Contracts include specific privacy protective clauses to prevent unauthorized access, use, disclosure and retention of PHI, with notification requirements to the CritiCall Privacy Lead for privacy breaches;
- Training for all employees, contracted workers, vendors, consultants, any other agents of HHS/CritiCall and hospitals that support the ongoing operation, management and maintenance of the Critical Care information System (CCIS);
- Execution of Confidentiality Agreements specifically for employees, contracted workers, vendors, consultants, and any other agents of HHS/CritiCall that support the ongoing operation, management and maintenance of the Critical Care information System (CCIS) outlining obligations for the safeguarding of PHI;
- A privacy program which begins with a comprehensive set of policies and procedures; and
- A governance structure in which privacy is represented has been set out in the *O1 – Privacy Governance and Accountability Framework* at the Senior Management level within HHS in respect of CCIS.

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). HHS/CritiCall provides a secure virtual private network (VPN) connection to the eHealth Ontario network to protect CCIS data from unauthorized access. HHS/CritiCall 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.

The CCIS is designed with role-based access controls so that only authorized users can access patient health and demographic information. For example, contributing hospital employees only have access to the clinical information of patients that they originally provided to HHS/CritiCall through CCIS.

HHS/CritiCall, in respect of the CCIS, conducts Network and Application Security Audits as well as Security Penetration Tests to assess the security of the CCIS application and its supporting infrastructure which include 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, Active Directory and Internet services) used to deliver the application. Security configuration of CCIS may be 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 may be 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.

Since HHS/CritiCall employees, contracted workers, vendors, consultants, any other agents of HHS/CritiCall and hospitals that support the ongoing operation, management and maintenance of the CCIS may have access to PHI on a daily basis, the following technical safeguards are enforced:

- A password policy which requires the use of strong passwords by employees which must be changed every 90 days;
- An acceptable use policy for HHS and CritiCall equipment; and
- A policy and procedure around the secure transfer of PHI.

Physical Safeguards

The Data Centre within which the CCIS is physically stored, is a vendor managed secure Data Centre in Streetsville, Ontario. The Data Centre has a security posture 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.

HHS provides a secure physical environment for those accessing the CCIS at CritiCall offices as set out in *S3 -Policy and Procedure for Ensuring Physical Security of Personal Health Information.* It includes but is not limited to the following physical security requirements:

- A secured perimeter accessible only by authorized persons;
- All laptop computers are encrypted and locked to the employee desk at all times when in use. When not in use, laptop computers must be stored in a secured location (e.g. a locked cabinet);
- All PHI stored for any period of time on a memory stick must be encrypted;
- All printed copies of PHI must be secured within a locked desk drawer or filing cabinet when not being used; and
- All visitors to the facility must enter through the main entrance and sign in/out during their visit. All visitors must be accompanied by an authorized HHS/CritiCall employee for the duration of their visit.

Principle 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 policies, procedures and practices for the collection, use, and disclosure of PHI via the CCIS available to all employees, agents, the general public, and participating hospitals. This information is available to the public upon request to the CritiCall Privacy Lead.

In addition, HHS ensures that the following information about the CCIS is readily available on their website:

- General information about HHS's information handling practices in respect of CCIS;
- A description of data HHS collects and retains; and
- Contact information on how reach the CritiCall Privacy Lead and the Information Privacy Commissioner of Ontario

HHS, in respect of the CCIS, provides materials to hospitals participating in the CCIS 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 visiting the CritiCall website at www.criticall.org or by contacting the CCIStrainingteam@criticall.org. These FAQs are also available to all CCIS users through the CCIS Document Library.

Enquiries for information about HHS privacy policies, procedures and practices in relation to the CCIS are immediately directed to the CritiCall Privacy Lead. The CritiCall Privacy Lead will respond to all enquires and escalate to the Director of Privacy and FOI, HHS, and the Executive Director, CritiCall as required. The CritiCall Privacy Lead may be contacted:

By email:

privacy@criticall.org

By Mail to:

Attention CritiCall Privacy Lead
1725 Upper James Street
Suite 200
L9B 1K7

By Telephone:

(289) 396-7000

In keeping with HHS's obligations as a Prescribed Person, CCIS privacy policies and practices are reviewed by the Information and Privacy Commissioner/Ontario every three years. Additional information on HHS and its privacy practices, as reviewed by the Information and Privacy Commissioner/Ontario, can be found at www.ipc.on.ca.

Principle 9 – Individual Access
Upon request, an individual shall be informed of the existence, use, and disclosure of his 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 own records of PHI, or to request amendments to their records of PHI in the CCIS, will be instructed to contact the CritiCall Privacy Lead, who in turn, will refer the patient to the physician or hospital that originally entered their PHI into the CCIS. These physicians or hospitals are responsible for providing patients with access to their PHI and for making corrections to a patient record. As HHS/CritiCall is also an 'institution' under the Freedom of Information and Protection of Privacy Act, Ontario, 1990 (FIPPA), access requests could also be made for Personal Information (PI) under FIPPA. If this is the case, HHS/CritiCall will transfer the request to the hospital which has collected the PI as that hospital may have the greater interest in the request and therefore would respond to the request.

Principle 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 CritiCall Privacy Lead:

By email to:

privacy@criticall.org

By mail to:

CritiCall Privacy Lead
1725 Upper James Street
Suite 200

L9B 1K7

By Telephone:

289-396-7000

The CritiCall Privacy Lead reviews all privacy concerns and complaints related to the CCIS. As warranted, the CritiCall Privacy Lead will conduct an investigation under the direction of the Director of Privacy and FOI, HHS, and take appropriate action including, as necessary, amending CCIS policies and procedures.

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

By mail to:

Information and Privacy Commissioner/Ontario
2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8.

By Telephone:

(416) 326-3333

Compliance

All employees, consultants, contracted workers, vendors or any other agent of HHS/CritiCall must comply with this policy and procedure.

If a breach of this policy is found to have occurred an investigation will conducted by the CritiCall Privacy Lead. If a breach, a potential breach or a privacy risk with regard to disclosure of PHI is identified by an employee, contracted worker, vendor, consultant, or any other agent of HHS/CritiCall, they must immediately contact the CCIS Help Desk. The Executive Director, CritiCall will be notified and require the CritiCall Privacy Lead to initiate a privacy investigation. Each investigation will follow the steps outlined within *P29 - Policy and Procedure for Privacy Breach Management.*

The HHS Director of Privacy and FOI, HHS or delegate and the CritiCall Privacy Lead will conduct an annual audit of this policy and procedure. The findings will be documented in the Log of Privacy Audits and presented to the CritiCall Executive Committee in an executive summary format. Identified mitigation tasks will be managed by the CritiCall Privacy Lead, documented in the Log of Privacy Audits and signed off by the HHS Director of Privacy and FOI. The HHS Director of Privacy and FOI or delegate may conduct additional random audits at any time.

GLOSSARY	
Terms Used in this Document	**Description**
Active Directory	A directory that includes all users of CritiCall information systems.
Admission, Discharge and Transfer	An information system that each hospital maintains that includes records of all admissions to, discharges from and transfers (within and external) of patients admitted to the hospital.
Agent	Agents may be employees, consultants, contracted workers, vendors or any other person who acts on behalf of HHS/CritiCall in respect of personal health information for the purposes of HHS/CritiCall and not the agent's own purposes, whether or not the agent has the authority to bind HHS/CritiCall and whether or not the agent is employed by the HHS/CritiCall and whether or not the agent is being remunerated.
Critical Care Response Team (CCRT)	A team that brings critical care expertise out of the ICU to patients throughout the hospital 24/7 to improve patient outcomes and efficiency of resource utilization.
Information and Privacy Commissioner/Ontario (IPC/O)	Information and Privacy Commissioner / Ontario is responsible for ensuring that government organizations, or those organization which are funded by government organization, comply with the access and privacy provisions of Ontario privacy legislation.
National Security Agency (NSA)	A cryptologic intelligence agency of the United States Department of Defense responsible for the collection and analysis of foreign communications and foreign signals intelligence, as well as protecting U.S. government communications and information systems, which involves information security and cryptanalysis/cryptography.
National Institute of Standards and Technology (NIST)	An agency based in the United States that develops and supplies industry, academia, government, and other users with '*standard reference materials'*. These artifacts are certified as having specific characteristics or component content, used as calibration standards for measuring equipment and procedures, quality control benchmarks for industrial processes, and experimental control samples.
Personal Health Information Protection Act, 2004	The Ontario health privacy statute which governs the manner in which personal health information may be collected, used and disclosed within the health care system.
Secure Socket Layer (SSL)	Is a commonly used protocol for managing the security of a message transmission on the internet. SSL uses the public and private key encryption system from RSA that includes the use of a digital certificate.

GLOSSARY	
Terms Used in this Document	**Description**
Virtual Private Network (VPN)	A network technology that creates a secure network connection over a public network such as internet or a private network owned by a service provider.

Summary of this Policy:	This policy outlines the privacy practices for HHS as a Prescribed Person in respect of CCIS under the *Personal Health Information Protection Act*, 2004 (PHIPA) as it relates to the collection, use and disclosure of personal health information (PHI).
Reference Documents:	MANUAL FOR THE REVIEW AND APPROVAL OF PRESCRIBED PERSONS AND PRESCRIBED ENTITIES Information and Privacy Commissioner/Ontario *P4 -Policy and Procedure for the Collection of Personal Health Information* *P5 - List of Data Holdings Containing Personal Health Information* *P7 - Statements of Purpose for Data Holdings Containing Personal Health Information* *P8 –Policy and Procedure for Limiting Agent Access to and Use of Personal Health Information* *P10 –Policy and Procedure for the Use of Personal Health Information for Research* *P13 - Policy and Procedures for the Disclosure of PHI for Research Purposes and the Execution of Research Agreements* *P19 –Policy and Procedure for the Execution of Data Sharing Agreements* *P24 -CCIS Policy and Procedure with Respect to De-Identification and Aggregation* *O1 – Privacy Governance and Accountability Framework* *S3 -Policy and Procedure for Ensuring Physical Security of Personal Health Information* *S5 -Policy and Procedure for the Secure Retention of Records of Personal Health Information* *S8-CCIS Policy and Procedure for the Secure Disposal of Records of Personal Health Information* *S14 –Policy and Procedure on the Acceptable Use of Technology*
Keyword Assignment:	Privacy, Policy, Prescribed Person, PHIPA and PHIPA Regulation, Principles, Safeguards
Policy Developed By:	Christine Moon, CritiCall Privacy Lead

In Consultation With:	Donna Thomson, Executive Director, CritiCall MaryWall, Director, Privacy and FOI, HHS Mark Farrow, Chief Security Officer, HHS Constantine Theofilopoulos, CritiCall Security Lead Swapna Petrelli, Associate Consultant, Healthtech Consultants Karen Waite, Associate Vice President, Healthtech Consultants