2020 REPORT TO THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO FROM HAMILTON HEALTH SCIENCES/CRITICALL ONTARIO IN RESPECT OF THE CRITICAL CARE INFORMATION SYSTEM

October 23, 2020

Table of Contents

Introduction

The Critical Care Information System (CCIS) is a comprehensive source of province-wide information on access to critical care, quality of care and outcomes for critical care patients in the province. The CCIS is a key component of the Ministry of Health's (the Ministry) critical care strategy for Ontario. Developed in 2006/2007, the CCIS was put in place in all Level 2 and Level 3 critical care units in Ontario hospitals. In 2017, the Ministry expanded the mandate of the critical care strategy to include neonatal intensive care units (NICUs), and the data collection for the CCIS was similarly expanded.

The purpose of the CCIS data holding is to enable analysis and statistical reporting of resource requirements, utilization and capacity in relation to patient acuity to enable evidenced based decision making to support system-wide capacity planning and targeted performance improvement initiatives. The CCIS provides the ability for system monitoring and managing the province's critical care resources more effectively, as well as identifying opportunities for implementing quality improvement initiatives at individual hospitals and across provincial regions.

The CCIS data set is comprised of personal health information (PHI) collected from Level 2 and Level 3 critical care units and neonatal critical care units (NICUs) at Ontario hospitals. It includes patient demographic data, data relating to admission sources, services provided, the associated date and times, admitting diagnoses, discharge destinations, health card numbers, medical record numbers, Critical Care Response Team and Paediatric Critical Care Response Team status, ventilator status, central venous and arterial line status, vasoactive/inotropic meds, intracranial pressure monitoring, pediatric logistic organ dysfunction, pediatric index of mortality, multiple organ dysfunction scores and continuous dialysis status. Data collected within the CCIS is limited to that which is necessary to fulfill the system's purpose.

Hamilton Health Sciences Corporation (HHS) is a prescribed person within the meaning of section 39(1) (c) of the Personal Health Information Protection Act (*PHIPA*) in respect of the CCIS. HHS operates the CCIS as part of its CritiCall Ontario ("CritiCall") program. Hospitals, or Health Information Custodians (HIC's) as defined in *PHIPA*, are permitted to disclose PHI to HHS through the CCIS without patient consent, provided HHS meets and continues to meet the requirements of the Information and Privacy Commissioner of Ontario (IPC) as they pertain to "Prescribed Persons."

Critical Care Services Ontario (CCSO), operated by the University Health Network (UHN), is appointed by the Ministry to develop the overall strategy for the CCIS, consistent with the CCIS purpose of supporting system wide critical care capacity planning and performance improvement. CCSO acts as an agent of HHS in regard to the analysis it performs on CCIS Data.

HHS/CritiCall's privacy and security practices in relation to the CCIS were approved by the IPC on October 31, 2014, and October 31, 2017, respectively. In order to continue to satisfy the PHIPA Regulations for "Prescribed Persons," HHS must provide a report to the IPC every three (3) years documenting the policies and procedures in place for protecting the privacy, confidentiality and security of patient information in the CCIS.

This report describes the privacy and security program in place at HHS, and more specifically at CritiCall, to support the requirements of the CCIS. This report is being submitted to satisfy the

requirements of section 13(2)(b) of the Regulation so that HHS can continue to act as a prescribed person in relation to the CCIS for the period of November 1, 2020 to October 31, 2023.

DEFINITIONS

"Authorized User" means an agent of a Participating Hospital who has been granted access to the CCIS to effect the disclosure, through electronic means, by the Participating Hospital to HHS/CritiCall for the purposes of the CCIS;

"Manual" means the IPC's Manual for the Review and Approval of Prescribed Persons and Prescribed Entities;

"Data Sharing Agreements" means the agreement established between HHS/CritiCall and Hospitals that enter data into the CCIS to authorize the collection, use and disclosure of this data for the purposes of the CCIS;

"Prescribed person", "a**gent**", "**collect**", "**use**", "**disclose**", "**health care**" and "**information practices**" each has the meaning ascribed to it in *PHIPA*;

"Third party service provider" means an agent that has been contracted by HHS/CritiCall to provide services that supports the ongoing operation of the CCIS.

PART 1 – PRIVACY DOCUMENTATION

The following section focuses on HHS's privacy policies and procedures as they relate to the CCIS. As CritiCall operates the CCIS on behalf of HHS, the policies and procedures are, in some cases, specific to the environment and staff in place at CritiCall, where the day-to-day activities related to the system take place. Overarching accountability continues to rest with the Chief Executive Officer of HHS and all participating hospitals contributing data to the CCIS are required to enter into agreements with HHS/CritiCall for the collection of CCIS data.

P1. PRIVACY POLICY IN RESPECT OF HHS AS A PRESCRIBED PERSON

HHS/CritiCall has developed and implemented an overarching privacy policy to protect the PHI collected through the CCIS. The policy is structured in accordance with the 10 key privacy principals and outlines how HHS/CritiCall attends to the specific responsibilities for each. This policy is available on CritiCall's website www.criticall.org and in the CCIS Document Library.

Status under the Act

This Privacy Policy describes the status of HHS/CritiCall as a prescribed person under *PHIPA* and the duties and responsibilities that arise as a result of this status. HHS has been prescribed by the Regulation 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, procedures and practices in place and reviewed and approved by the IPC every three (3) years. For HHS, this is to protect the privacy and confidentiality of the PHI within the CCIS.

This overarching Privacy Policy indicates that HHS/CritiCall has implemented policies, procedures and practices to protect the privacy of individuals whose PHI it receives and to maintain the confidentiality of that information. This overarching Privacy Policy demonstrates HHS's commitment, as a prescribed person, to comply with the provisions of *PHIPA*, its Regulation and the ten (10) privacy principles found in the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information.

Privacy and Security Accountability Framework

This Privacy Policy clearly indicates that the HHS CEO is ultimately accountable for ensuring compliance with PHIPA and all HHS obligations as a prescribed person in relation to the CCIS. This Privacy Policy indicates that the HHS Chief Privacy[1] Officer, jointly with the CritiCall Executive Director, have been delegated to oversee compliance with the Act, its Regulation, and ensuring compliance with the CCIS privacy and security policies, procedures and practices.

This Privacy Policy states that the CritiCall Executive Director has appointed a CritiCall Privacy Lead who is responsible for the day-to-day privacy operations, compliance and management and a CritiCall Security Lead who is responsible for ensuring PHI managed via CCIS hardware and

[1] In addition to HHS' CPO, a full-time Privacy Lead role was on-boarded at CritiCall Ontario in June 2018 to support the CCIS and other programs under CritiCall Ontario.

software is secure and maintained in compliance with the CCIS security policies. Both report directly to the CritiCall Executive Director.

This Privacy Policy identifies the CCIS Data Stewardship Committee as being responsible for overseeing the CCIS data holding and receives reports on all issues that impact the CCIS data holding and requests for CCIS data.

A formal HHS/CritiCall Committee oversees HHS/CritiCall's privacy practices. The Committee receives reporting on all issues that impact the CCIS data holding and provides a forum to ensure consistency in privacy practices across HHS/CritiCall.

Collection of Personal Health Information

This privacy policy states that HHS/CritiCall must ensure that each collection identified in this policy is consistent with the collections of PHI permitted by the Act and its Regulation. The policy states that HHS/CritiCall collects PHI (i.e. critical care data) from HICs through the CCIS 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 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. This privacy policy requires that HHS/CritiCall collect only the PHI that is necessary to fulfill its mandate and consistent with the collections of PHI permitted by the Act and its regulation. This privacy policy includes procedures and practices that ensure that both the amount and type of PHI collected is limited to only what is necessary.

This privacy policy indicates that the benefits and the purpose for collection are to be communicated to all CCIS end users through the CCIS Data Collection Guide and the CCIS Instructional Guide distributed to participating CCIS hospitals. The participating hospitals' staff responsible for entering data into the CCIS also receive information about the purpose of the collection through a mandatory privacy module within the CCIS. This module was added in March 2016 and is mandatory for all authorized new CCIS users and must be completed annually by all authorized CCIS users.

Additionally, data sharing agreements between each participating hospital and HHS/CritiCall, with respect to the CCIS clearly outline the purpose of data collection.

The purposes for which HHS/CritiCall collects PHI is explained 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.

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

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 CCIS is not a free-text system; radio buttons and drop down selections exist to limit the amount of data collected. The policy describes the type of data collected which includes data in the categories of patient demographics; patient data; adult and paediatric Critical Care Response Team (CCRT) (PCCRT) status; bed availability; and life support interventions.

This privacy policy includes a full listing of data holdings of PHI maintained by the HHS/CritiCall and directs individuals to the data elements/data sources for those data holdings found in *P5: List of Data Holdings Containing Personal Health Information* and *P7: Statements of Purpose for Data Holdings Containing Personal Health Information*, to obtain further information in relation to the purposes, data elements and data sources for each data holding of PHI.

Use of Personal Health Information

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. This privacy policy identifies the purposes for which PHI is used and distinguishes that aggregate or de-identified information be used in place of PHI if it can serve the purpose. This privacy policy and procedures distinguishes between the use of PHI and the use of de-identified and/or aggregate information and between the use of PHI for purposes of subsection 39(1)(c) or section 45 of the Act, as the case may be, and the use of PHI for research purposes.

This privacy policy states that HHS/CritiCall uses the PHI to create aggregate level reports on bed availability, critical care services and patient outcomes. PHI from the CCIS may also be requested and used for research provided the conditions of section 44 of *PHIPA* are met. Release of PHI for research is considered a "disclosure" and policies and procedures are in place to facilitate the approval or denial of these requests as deemed appropriate by the CCIS Data Stewardship Committee based on the purpose of the data collection and compliance with *PHIPA*.

This privacy policy states that HHS/CritiCall will not use PHI if other information will serve the purpose and will not use more PHI than is reasonably necessary to meet the purpose and that the use will be consistent with PHIPA and its regulation.

For planning purposes, HHS/CritiCall uses PHI collected from Ontario hospitals through the CCIS to create aggregate level reporting on bed availability, critical care service utilization and patient outcomes. These reports do not contain any PHI and are provided to the MOHLTC, Local Health Integration Networks (LHINs) and hospitals to facilitate the allocation of resources and funds for improving critical care services in Ontario.

The privacy policy states that the prescribed person remains responsible for the PHI used by its agents at Principle 5.

The privacy policy also states that HHS/CritiCall has developed policies, procedures and agreements that limit the activities of agents and the collection, use, disclosure, retention and disposal of personal health information, in accordance with *PHIPA* and its regulation. The privacy policy identifies the policies, procedures and practices implemented to ensure that its staff and other agents only collect, use, disclose, retain and dispose of PHI in compliance with *PHIPA* and its regulation and in compliance with the privacy and security policies, procedures and practices implemented. HHS/CritiCall also uses role-based access controls that restrict the types of information that may be used by HHS/CritiCall employees and other agents to perform their duties in relation to the CCIS.

Roles and access are assigned on a "need-to-know basis" in accordance with the duties to be performed by the agent.

Disclosure of Personal Health Information

The privacy policy states that HHS/CritiCall will not disclose any PHI if other information will serve the purpose and will not disclose more PHI than is reasonably necessary to meet the purpose for the permitted disclosure. The privacy policy clearly distinguishes between the purposes for which and the circumstances in which PHI is disclosed.

The privacy policy indicates that the following are circumstances in which HHS/CritiCall 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/CritiCall 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/CritiCall stipulating the terms for the use, disclosure, security, return, or disposal of the PHI disclosed by HHS/CritiCall 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 for 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).

The privacy policy clearly distinguishes between the purposes for which and the circumstances in which PHI is disclosed; as well as the circumstances in which and the purposes for which de-identified and/or aggregate information is disclosed.

The privacy policy requires that HHS/CritiCall ensures that any disclosure of PHI is permitted by PHIPA and its regulation and is done in a manner consistent with PHIPA and its regulation.

The privacy policy requires that HHS/CritiCall review all de-identified and/or aggregate information prior to its disclosure and 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.

HHS/CritiCall discloses aggregate statistical reports and trended indicator reports for critical care planning purposes. Patient specific information is not included in these aggregate reports. Reports are available to the MOHLTC, LHINs, Critical Care Services Ontario (CCSO) and participating hospitals and provide vital decision making analysis to improve resource allocations for critical care patients. All aggregate reporting is reviewed prior to its disclosure to ensure no PHI is included and 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 Procedures with Respect to De-Identification and Aggregation.*

Secure Retention, Transfer and Disposal of Records of Personal Health Information

This privacy policy includes the requirements for secure retention of records of PHI in both paper and electronic format, including how long records of PHI are retained, whether the records are retained in identifiable form and the secure manner in which they are retained. The policy also addresses the manner in which records of personal health information in both electronic and paper format will be securely transferred and disposed of.

The privacy policy states that PHI collected from the CCIS is currently retained for as long as is reasonably necessary to fulfill the purpose for which it was collected and in the least identifiable form possible. Critical care aggregate reports generated by HHS/CritiCall are retained indefinitely for historical analysis purposes.

This privacy policy requires that HHS/CritiCall only receives PHI in electronic format. This privacy policy requires electronic data to be 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 participating hospitals is retained in an electronic format within the CCIS and in accordance with the '*S5 -Policy and Procedures for the Secure Retention of Records of Personal Health Information'*. The policy states that any disposal of PHI retained within the CCIS must comply with the '*S8: CCIS Policy and Procedures for the Secure Disposal of Records of Personal Health Information*.' Additionally, the policy states that any CCIS equipment that is replaced or retired will be destroyed in accordance with *S8: CCIS Policy and Procedures for the Secure Disposal of Records of Personal Health Information*.

It is not the practice of HHS/CritiCall employees or agents assigned to support the CCIS to print or use paper copies of PHI from the CCIS, however; all agents are responsible for permanently destroying (e.g. through irreversible shredding) any PHI printed from the CCIS once the information is no longer required in accordance with '*S8: CCIS Policy and Procedures for the Secure Disposal of Records of Personal Health Information*.' PHI in paper form must also be secured at all times, as stated in *S3: Policy and Procedures for Ensuring Physical Security of Personal Health Information*.

Implementation of Administrative, Technical and Physical Safeguards

This privacy policy requires that HHS/CritiCall has administrative, technical, and physical safeguards in place to protect PHI in the CCIS against loss or theft, unauthorized access, disclosure, copying, use, disposal or modification. These safeguards apply to PHI in paper or electronic form.

Inquiries, Concerns or Complaints Related to Information Practices

This privacy policy states that 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 participating hospital that originally entered their PHI into the CCIS. These 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 participating hospital which has collected the PI as that hospital may have the greater interest in the request and therefore would respond to the request.

This privacy policy identifies to whom and the manner in which individuals may direct inquiries, concerns or complaints related to HHS/CritiCall's privacy policies, procedures and practices about the CCIS or about the compliance of HHS/CritiCall with *PHIPA* and the Regulation. This information is also available to the public on CritiCall's website.

Individuals can submit their privacy concerns or complaints regarding the CCIS to the CritiCall Privacy Lead by telephone or in writing. Contact information for the CritiCall Privacy Lead including title, mailing address, email address is updated and maintained in the Privacy section of CritiCall Ontario's website. All privacy concerns and complaints related to the CCIS will be reviewed by the CritiCall Privacy Lead, and as warranted, the CritiCall Privacy Lead will conduct an investigation under the direction of the HHS Chief Privacy Officer.

This privacy policy also indicates that individuals may also make a privacy complaint about the compliance of HHS/CritiCall, with the *Act* and its Regulation, directly to the IPC. Contact information, including mailing address, for the IPC is maintained on the CritiCall website and in the privacy policy.

Transparency of Practices in Respect of Personal Health Information

This privacy policy indicates that HHS/CritiCall shall make information about its privacy policies, procedures and practices for the collection, use, and disclosure of PHI through the CCIS available to all employees, agents, the general public, and participating hospitals. All policies, procedures and related documents are available to participating hospitals and their authorized CCIS users through the CCIS Document Library. The privacy policy further states that HHS ensures the following information about the CCIS is maintained and readily available on the CritiCall website:

- General information about HHS/CritiCall's information handling practices in respect of the CCIS;
- A description of data HHS/CritiCall collects and retains for the CCIS;
- CCIS Frequently Asked Questions;
- HHS/CritiCall Ontario Statement of Information Practices for the CCIS; and
- Contact information on how to reach the CritiCall Privacy Lead and the IPC is available including: the name and title of the contact person, mailing address and contact information for the agent to whom inquiries, concerns or complaints may be directed to and the manner and format in which these inquires, concerns or complaints may be made.

In keeping with HHS's obligations as a Prescribed Person, CCIS privacy policies and practices are reviewed by the IPC every three (3) years. Additional information on HHS and its privacy practices, as reviewed by the IPC, can be found at www.ipc.on.ca.

P2. POLICY AND PROCEDURES FOR ONGOING REVIEW OF PRIVACY POLICIES, PROCEDURES AND PRACTICES

HHS/CritiCall has developed and implemented a policy and procedure for the ongoing review of the privacy policies, procedures and practices put in place. This privacy policy requires HHS/CritiCall to have ongoing review of privacy policies, procedures and practices. This privacy policy indicates that the CritiCall Privacy Lead is responsible for initiating, managing and documenting the completion of the annual policy and procedures review process. The purpose of the review is to determine whether amendments and/or new privacy policies, procedures and practices are necessary. Consideration must be given a number of factors during the review including: any Orders, decisions, guidelines, fact sheets and best practices issued by the IPC under *PHIPA* and its Regulation; evolving industry privacy standards and best practices; amendments to *PHIPA* and its Regulation relevant to HHS/CritiCall; and recommendations arising from privacy audits, privacy impact assessments and investigations into privacy complaints, and privacy breaches.

This privacy policy requires that the review must also assess whether the privacy policies, procedures and practices of HHS/CritiCall for the CCIS continue to be consistent with actual practices and whether there is consistency between and among the privacy and security policies, procedures and practices implemented for the CCIS.

The annual review is conducted in the spring of each year with the CritiCall Privacy Lead providing a report to the CritiCall Executive Director and the HHS Chief Privacy Officer advising of the findings and recommendations by June 30th of each year. The CritiCall Executive Director and the Chief Privacy Officer review the findings and provide direction for the revision of existing policies, procedures or practices or the development of new policies, procedures or practices by August 31 of each year. Details related to the review of privacy policies, procedures and practices related to the CCIS are included in Part 5 of this report.

The Privacy Lead is responsible for drafting any new privacy policies, procedures and practices if deemed necessary as a result of the review. Once drafted, the policies, procedures and practices will be sent first to the Executive Director, CritiCall Ontario, then to the HHS Chief Privacy Officer for review. The policy states that approval authorities may request that any policy, procedure or practice be reviewed by an additional relevant individual or group prior to granting approval.

This privacy policy requires that any new or amended privacy policies, procedures or practices in relation to CCIS are communicated to all entities and individuals involved in the operational planning and day-to-day activities of the CCIS by way of written correspondence and/or via electronic means such as email. The CritiCall Privacy Lead works in conjunction with the CritiCall Executive Director, the HHS Chief Privacy Officer and the CCIS Education Team to coordinate communications. The CritiCall Privacy Lead is also responsible for updating any communication material in relation to the new or amended policies procedures or practices.

This privacy policy and procedures states CritiCall Executive Director is responsible for enforcing compliance and that all HHS/CritiCall employees and agents must comply with this policy and its procedures.

The CritiCall Privacy Lead is responsible for conducting an annual audit of compliance with this policy and procedures in accordance with the *Policy and Procedures in Respect of Privacy Audits* and/or HHS/CritiCall's *Policy and Procedures for Ongoing Review of Security Policies, Procedures*

and Practices. Audit findings are reported to the CritiCall Executive Director and the HHS Chief Privacy Officer.

If a breach of this policy is found to have occurred, an investigation will be conducted by the CritiCall Privacy Lead. If a breach, a suspected breach or a privacy risk with regard to disclosure of PHI is identified by an employee or any other agent of HHS/CritiCall they must immediately contact the CCIS Help Desk. The CritiCall Executive Director will be notified and require the CritiCall Privacy Lead to initiate a privacy investigation in accordance with *P29: Policy and Procedures for Privacy Breach Management*.

P3. POLICY ON THE TRANSPARENCY OF PRIVACY POLICIES, PROCEDURES AND PRACTICES

HHS/CritiCall has developed and implemented a policy and procedures on the transparency of privacy policies, procedures and practices. This policy and associated procedures states that HHS/CritiCall must make information about its privacy policies, procedures and practices, available to the public and other CCIS stakeholders. This policy requires that the following information is available to the public: HHS/CritiCall's privacy policies and procedures; brochures or frequently asked questions related to the privacy policies, procedures and practices implemented by HHS/CritiCall; documentation related to the three (3) year review by the IPC; a list of data holdings of PHI maintained by HHS/CritiCall; and the name and/or title, mailing address and contact information of the agent(s) to whom inquiries, concerns or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with the Act and its regulation may be directed.

This privacy policy outlines the minimum content of brochures or frequently asked questions including the status of HHS under *PHIPA*, the duties and responsibilities arising from this status, and the privacy policies, procedures and practices implemented in respect of PHI, including: the types of PHI collected and the persons or organizations from which this PHI is typically collected; the purpose for which it is typically collected; the purposes for which PHI is used, and if identifiable information is not routinely used, the nature of the information that is used; and the circumstances in which and the purposes for which PHI is disclosed and the persons or organizations to which it is typically disclosed.

This privacy policy and procedures also requires that brochures or frequently asked questions identify some of the administrative, technical, and physical safeguards implemented to protect the privacy of individuals whose PHI is received and to maintain the confidentiality of that information, including the steps taken to protect PHI against theft, loss, and unauthorized use of disclosure and to protect records of PHI against unauthorized copying, modification or disposal.

HHS/CritiCall provides open and transparent access to general outlines of existing policies, procedures and practices, as appropriate. An overview of the privacy practices related to the CCIS are posted on the privacy section of the CritiCall website. The following information in relation to the CCIS is also accessible on the CritiCall website: summaries of all Privacy Impact Assessments (PIAs), a list of Frequently Asked Questions (FAQ's) about the HHS/CritiCall privacy practices in relation to CCIS and the response to each question.

The CritiCall Privacy Lead is the contact for all inquiries, concerns or complaints related to compliance with privacy policies, procedures and practices and compliance with *PHIPA* and its Regulation. Full contact information for the CritiCall Privacy Lead and the IPC is available in the privacy section of CritiCall's website.

All privacy policies and procedures are available in the CCIS Document Library to participating hospitals' authorized users and HHS/CritiCall employees and agents, as well as, upon request to the CritiCall Privacy Lead.

P4. POLICY AND PROCEDURES FOR THE COLLECTION OF PERSONAL HEALTH INFORMATION

HHS/CritiCall has developed and implemented this policy and procedures governing the collection of PHI.

This policy outlines how HHS/CritiCall identifies the purposes for which PHI will be collected, the data elements collected, from whom the PHI may be collected and the safeguards around the transfer of that PHI to the CCIS.

This privacy policy states that HHS/CritiCall collects a standard set of data elements, including PHI, from Ontario hospitals participating in the CCIS. The data elements and purpose of this collection are described in detail in *P5: List of Data Holding* and *P7: Statement of Purpose for Data Holdings Containing Personal Health Information*. This privacy policy requires that data collection is limited to that which is permitted by the *PHIPA* and reasonably necessary to meet the purpose for the collection. As indicated in this privacy policy, HHS/CritiCall is committed to not collecting PHI in respect of CCIS if other information will serve the same purpose and will limit the collection of PHI in respect of the CCIS to that which is reasonably necessary to meet the purpose.

The privacy policy requires that all HHS/CritiCall agents must comply with this policy and states that the Executive Director, CritiCall, is responsible for enforcing compliance. This privacy policy details that the HHS Chief Privacy Officer, or delegate and the CritiCall Privacy Lead will conduct an annual audit of this policy and procedure. This privacy policy requires the audit to be conducted in accordance with the *Policy and Procedures in Respect of Privacy Audits*.

This policy and procedures further requires that agents notify HHS/CritiCall at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy and procedures.

This policy addresses the consequences of a breach. If a breach is found to be intentional or the result of continuous negligent work practices, the policy provides that disciplinary action will be taken up to and including termination of employment and/or laying criminal charges, as per *H11: Policy and Procedures for Discipline and Correction Action.*

Review and Approval Process

This privacy policy states that in advance of any new implementation of the CCIS within a hospital not yet participating in the CCIS, the CCIS Product Manager will notify the CritiCall Privacy Lead.

The CritiCall Privacy Lead is responsible for reviewing requests and determining if the implementation is in line with all other implementations and shall consider whether other data, namely de-identified and/or aggregate information, will serve the identified purpose. This includes ensuring the data elements to be collected are the same as those currently being collected from other participating hospitals; the collection is permitted by *PHIPA* and its Regulation; the amount of PHI is limited to that which is necessary to meet the purpose identified; and there is no conflict with existing CCIS privacy or information security policies and procedures. All hospitals with critical care units contributing data to the CCIS must enter into an agreement with HHS/CritiCall prior to contributing data. As a condition of approval prior to participation in the CCIS, the CritiCall Privacy Lead will determine if agreements are in place or need to be executed prior to the implementation.

As outlined in this privacy policy, the CritiCall Privacy Lead is responsible for communicating the decision via electronic correspondence to the party requesting implementation of the CCIS.

Conditions or Restrictions on the Approval

This privacy policy identifies the conditions or restrictions that are required to be satisfied prior to the collection of PHI, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) responsible for completing, providing or executing the documentation and/or agreements. The policy further requires that conditions or restrictions have regard to the requirements of the Act and its regulation.

The CritiCall Privacy Lead will document any conditions or restrictions for the collection. The CritiCall Privacy Lead will provide a reason for the decision, conditions and safeguards and forward the document to the CCIS Product Manager, the CritiCall Executive Director and, in the event that new data elements are being requested for collection, to the CCIS Data Stewardship Committee.

The CCIS Product Manager will provide the CritiCall Privacy Lead with the documents required to show compliance with all conditions and restrictions outlined in the decision document. The CritiCall Privacy Lead shall ensure all restrictions and conditions are satisfied prior to the collection of any new PHI.

Secure Retention

This privacy policy requires that PHI collected through the CCIS is retained in a secure manner and in compliance with *S5: Policy and Procedures for Secure Retention of Records of Personal Health Information* and only for as long as necessary to fulfill the purpose for which it was collected and in the least identifiable form possible. All PHI shall be retained in compliance with *S8: Policy and Procedure for Secure Disposal of Records of Personal Health Information.*

Secure Transfer

This privacy policy requires that if PHI is being collected by an agent of HHS/CritiCall, that the records be transferred in a secure manner in compliance with *S7: Policy and Procedures for Secure Transfer of Records of Personal Health Information.* Electronic data is securely transferred into the CCIS through a 256 bit secure VPN connection over the eHealth Ontario network.

Secure Return or Disposal This privacy policy states that if records of PHI are to be destroyed or returned following the retention period as set out in any documentation and/or agreements executed prior to the collection of the PHI, that the CritiCall Privacy Lead is responsible for ensuring that records of PHI are either securely returned or disposed of and that the destruction shall occur in compliance with *S8: Policy and Procedures for Secure Disposal of Records of Personal Health Information*.

This privacy policy outlines in what circumstances records are securely returned to the person or organization from which they were collected. This privacy policy requires these records to be transferred in a secure manner and in compliance with *S7: Policy and Procedures for Secure Transfer of Records of Personal Health Information.*

P5. LIST OF DATA HOLDINGS CONTAINING PERSONAL HEALTH INFORMATION

HHS/CritiCall has developed and maintains an up-to-date list of data holdings containing PHI. HHS/CritiCall maintains one data holding. The CCIS Data Holding is comprised of standard critical care data elements. The list of data elements included in the CCIS Data Holding and statement of purpose for the CCIS Data Holding are combined in a single document. The PHI collected includes: Medical Record Number (MRN); Name (first, middle, last); Year, Month of Birth and Date of Birth; Gender; Health Card Number; Health Card Type; Health Card Version Code; and Age.

The CCIS data holding is comprised of standard critical care data elements entered into the CCIS by authorized individuals employed by critical care units in participating Ontario hospitals. The purpose of the CCIS data holding is to enable analysis and statistical reporting of resource requirements, utilization and capacity in relation to patient acuity to further enable evidenced based decision making to support system-wide capacity planning and targeted performance improvement initiatives. Data collected within the CCIS is limited to that which is necessary to fulfill the above purpose.

HHS/CritiCall provides aggregate statistical reports and trended indicator reports to the MOHLTC, LHINS, Critical Care Services Ontario and hospitals for critical care planning purposes. These reports do not contain patient specific information. 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 Procedures with Respect to De-Identification and Aggregation.*

P6. POLICY AND PROCEDURES FOR STATEMENTS OF PURPOSE FOR DATA HOLDINGS CONTAINING PHI

HHS/CritiCall has developed and implemented a policy and procedures for statements of purpose for the data holdings containing PHI. This privacy policy requires that HHS/CritiCall maintains, reviews and updates as necessary, a statement of purpose document for the CCIS data holding which must include the purpose of the data holding; a list of all PHI data elements contained within the data holding and the statements of purpose set out the need for the PHI in relation to the purpose; and the

source of the PHI data elements. This privacy policy and procedures identifies the CritiCall Privacy Lead as responsible for the day-to-day management of the privacy program.

This privacy policy identifies the people and organizations that will be provided the statements of purpose and, at a minimum, this privacy policy requires that the HICs and other persons or organization from whom the PHI in the data holding is collected be provided the statements of purpose.

Creation of Statements of Purpose

This privacy policy provides that the CCIS Data Set is a comprehensive listing of all data elements found within the CCIS. An advisory group developed and approved the data set based on patient safety concerns and improved resource access considerations.

This privacy policy and procedure identifies the CCIS Product Manager, under the direction of the CritiCall Privacy Lead, as the responsible person for creating the statements of purpose. This statement is reviewed and approved by the CCIS Data Stewardship Committee to ensure the collection of PHI is consistent with the HHS/CritiCall mandate in relation to the CCIS. The process to be followed in completing the statements of purpose are included in this privacy policy and procedures.

Review of Statements of Purpose

This privacy policy requires that the CritiCall Privacy Lead and the CCIS Product Manager review the statements of purpose whenever any new data elements are considered for collection. This policy also includes the process that must be followed when reviewing and amending the statements of purpose. However, if no changes in the data elements are made within a 12-month period, a review of the CCIS Data Set shall be conducted by the CritiCall Privacy Lead to ensure the data elements in the list are still accurate and the items listed are still required in order to fulfill the purpose.

The CCIS Data Set will be reviewed by the CCIS Data Stewardship Committee at least one time within every 12-month period. This privacy policy and procedures outlines the persons and organizations that will receive notice or copies of the amended statements of purpose including but not limited to health information custodians or other persons or organizations from whom the PHI data holding is collected.

Amendment of the Statements of Purpose

This privacy policy states that in order to determine if the current data elements in the CCIS Data Set are accurate and necessary, the CritiCall Privacy Lead, the CCIS Product Manager and the CritiCall Manager Business Innovation and Reporting shall confirm that each data element identified within the CCIS Data Set is still required in order to produce critical care reports. If any data elements within the CCIS Data Set are to be removed, a Recommendation Briefing Note will be created outlining the reason for the removal of the data element. The change must be reviewed by the CritiCall Manager, Information Technology to confirm its impact to the operation of the CCIS application. The final approval shall be given by the CritiCall Executive Director after review by the CCIS Data Stewardship Committee.

Amendments to the statement of purpose, as noted within the CCIS Data Set shall be posted on the CCIS section of the HHS/CritiCall website. Amendments that change the amount of PHI collected from a participating hospital will be reviewed with the hospitals and may result in an amendment to Data Sharing Agreements.

Compliance

This privacy policy requires all HHS/CritiCall employees and agents to comply with this policy. This privacy policy and procedures provides that the CritiCall Privacy Lead is responsible for enforcing compliance and this privacy policy outlines the consequences of a breach. This privacy policy stipulates that compliance will be audited in accordance with P27*: Policy and Procedures In Respect of Privacy Audits*.

This privacy policy and procedures requires the HHS Chief Privacy Officer, or delegate and the CritiCall Privacy Lead to conduct an annual audit for ensuring compliance with this privacy policy and procedures.

The privacy policy requires that if a breach, potential breach or privacy risk, with regards to the creation, review amendment and approval of the Statement of Purpose is identified by an agent that they are required to notify the Privacy Lead immediately. In addition, if a breach of this policy is found to have occurred, an investigation will be conducted by the CritiCall Privacy Lead.

P7. STATEMENTS OF PURPOSE FOR DATA HOLDINGS CONTAINING PERSONAL HEALTH INFORMATION

HHS/CritiCall maintains a statement of purpose for the CCIS Data Holding. This statement of purpose explains the purpose and goals of the data holding; the PHI contained; the sources of the PHI; and the need for the PHI in relation to the identified purpose and is combined with *P5 – List of Data Holdings Containing PHI.*

P8. POLICY AND PROCEDURES FOR LIMITING AGENT ACCESS TO AND USE OF PERSONAL HEALTH INFORMATION

HHS/CritiCall has developed and implemented a policy and procedures for limiting agent access to and use of PHI.

Limiting Agent Access to and Use of Personal Health Information Policy

This policy and procedures outlines how HHS/CritiCall employees and other agents, shall ensure that access and use of PHI is limited to the least identifiable information and only the information required for carrying out day-to-day employment, contractual or other CCIS related responsibilities. This privacy policy and procedures identifies the limited and narrowly defined purposes for which and circumstances in which agents are permitted to access and use PHI and the levels of access to PHI that may be granted.

This privacy policy indicates that HHS/CritiCall shall limit access to PHI by HHS/CritiCall employees and any other agents of HHS/CritiCall to ensure that PHI is only used on a "need-to-know basis" in order to perform their duties in relation to the CCIS.

This privacy policy and procedures explicitly prohibits access to and use of PHI if other information, such as de-identified and/or aggregate information, will serve the identified purpose and prohibits access to or use of more PHI than is reasonably necessary to meet the identified purpose. This privacy policy requires agents to access and use de-identified and/or aggregate information, as defined in HHS/CritiCall's *Policy and Procedures with Respect to De-Identification and Aggregation*, when agents are not permitted to access and use PHI.

This privacy policy and procedures requires that the duties of any agent with access to PHI are segregated in order to avoid a concentration of privileges that would enable a single agent to compromise PHI.

Review and Approval of Access

This privacy policy outlines that access privileges are assigned across multiple business units on a "need-to-know" basis and only if other information such as de-identified and/or aggregate information will not be sufficient to meet the HHS/CritiCall CCIS mandate. In such cases, access is granted to the least amount of PHI necessary for the CCIS group or role. This privacy policy also indicates that there are different levels of access to the CCIS based on the agent's role. The policy outlines the procedure to be followed.

This privacy policy and procedures identifies the agent(s) responsible and the process to be followed in receiving, reviewing and determining whether to approve or deny a request by an agent for access to and use of PHI along with the various level(s) of access that may be granted by HHS/CritiCall. . This privacy policy indicates that there are three (3) levels of access to PHI based on the "need to know" principle: (1) Admin.; (2) Support; and (3) Audit. Each access level has corresponding restrictions and conditions with respect to accessing PHI. The process for determining the appropriate access level is also identified in this privacy policy and procedures.

This policy and procedures outlines the process to be followed and sets out the requirements to be satisfied in requesting, reviewing and determining whether to approve or deny a request by an agent for access to and use of PHI; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

When any person requires access permissions to CCIS and requires access to the PHI within the CCIS, the Authorized User requesting access to PHI must meet with a supervisor/manager to discuss same. The supervisor/manager must be satisfied that the identified purpose for which the person requires access cannot be satisfied without the PHI. The person requesting access is required to complete a *CCIS Access to PHI Request Form*.

This policy and procedures indicates that once the request form is completed, the form must be approved by each of the following managers: CCIS Product Manager; CritiCall Privacy Lead; CritiCall Manager, Information Technology; and CritiCall Executive Director. In determining whether to approve or deny a request for access to a use of PHI and, if the request is approved, the

criteria that must be considered in determining the appropriate level of access, the managers must use the following criteria:

- Does the employee, agent or vendor require and use PHI on an ongoing basis or for a specific period of time?
- Is the request linked to the fulfillment of employment or contractual obligations for the CCIS?
- Is the purpose for access and use, given by the requestor, in compliance with PHIPA and its Regulation?
- Can the same purpose be achieved with de-identified or aggregate information?
- Is access to and use of PHI the only way to accomplish the duties of the requestor, as they relate to the CCIS mandate?
- Is the Access Level requested appropriate so that no more PHI than is reasonably necessary will be accessed and used to meet the identified purpose?

Each manager is required to record their comments and approval or denial of the request. They will also identify any conditions that must be met prior to granting access for the use of PHI. The form is then forwarded to the Manager, Information Technology to determine final approval. If approved, he/she will email the requestor and their supervisor/manager to advise that either:

- An approval has been granted; or
- The request has been denied, or a condition must be met, or documentation provided before access will be granted.
- All signed forms shall be saved on the HHS/CritiCall document repository (SharePoint).

HHS/CritiCall employees, agents and vendors that are not granted access to the PHI in CCIS may use de-identified or aggregate information, as defined in *P24: CCIS Policy and Procedures with Respect to De-Identification and Aggregation.* De-identified or aggregate information is available for internal use only, unless formally approved for release by the Executive Director, CritiCall as defined in *P24: CCIS Policy and Procedures with Respect to De-Identification and Aggregation.*

This privacy policy states that HHS/CritiCall employees, agents and vendors are prohibited from using de-identified and/or aggregate information, either alone or with other information available to them, in order to identify an individual. This includes any attempt to purposefully:

- Decrypt information that is encrypted;
- Identify an individual based on unencrypted information; and
- Identify an individual based on prior knowledge.

Conditions or Restrictions on the Approval of Access

This privacy policy and procedures identifies the conditions or restrictions imposed on an agent granted approval to access and use PHI, such as read, create, update or delete limitations, and the circumstances in which the conditions or restrictions will be imposed. The policy and procedures prohibits an agent granted approval to access and use PHI from accessing and using PHI except as necessary for his or her employment, contractual or other responsibilities; from accessing and using PHI if other information will serve the identified purpose; and from accessing and using more PHI than is reasonably necessary to meet the identified purpose. HHS/CritiCall ensures that all accesses to and uses of PHI are permitted by the Act and its regulation.

This privacy policy provides for the following conditions and restrictions, which may be applied to employee, agent and vendor accounts to ensure the appropriate access controls are in place for continuous monitoring and safeguarding of PHI within the CCIS.

1. **Access Level Restrictions**

2. These are imposed on CCIS users through the Access Level granted. The actions that various assigned levels can perform on PHI may include the ability to read, create, update or delete the PHI within CCIS. **Expiry of Access Privileges**

In accordance with this privacy policy, all Authorized Users will be subject to an expiry of access privileges to PHI for CCIS accounts. The expiry period will be assigned at the time of access initiation for the term of one (1) year maximum. If access to PHI is required for a shorter period of time, the date for the termination of the privileges will be set at the time of access initiation. This privacy policy and procedures identifies the process for ensuring that access to and use of PHI is permitted only for a specified time period. Access to and use of PHI are permitted only in accordance with *PHIPA* and its Regulation.

3. **Use of Personal Health Information**

Authorized Users with access and use privileges must accept the terms of the CCIS Confidentiality Agreement which states that those authorized to access and use PHI are prohibited from accessing and using more PHI than is reasonably necessary to meet the purpose for which they have been given access; to only that which is permitted by *PHIPA* (as per the approved *CCIS Access to PHI Request Form*); and to that which is required by the user to fulfill their employment or contractual purpose. Prior to accessing PHI, all users will make every effort to use information that is either de-identified or aggregated, whenever possible.

Roles that Access Personal Health Information

The following table identifies the groups/roles that support the CCIS mandate and require access to personal health information, the purpose for the access to PHI and their corresponding Access Level.

Group/Roles	Purpose for Access to Personal Health Information from CCIS	Access Level
CCIS Product Manager	Requires functionality to discharge oversight responsibilities including: CCIS Help Desk Lead, Technical Lead, Application Lead, HL7 Lead	1 (Admin) and 2 (Support)
CCIS Help Desk	Requires functionality to discharge operational support duties.	1 (Admin) and 2 (Support)
CCIS Audit Officer	Requires functionality to perform audits as set out in HHS/CritiCall policy.	3 (Audit)

Group/Roles	Purpose for Access to Personal Health Information from CCIS	Access Level
CCIS Training Team/Educators	Requires functionality to provide real-time on-site individual user support on demand.	2 (Support)
Datavail Solution Architect	Requires functionality to provide second level support and only if directed.	2 (Support)

Restrictions on Disclosures of Personal Health Information

This privacy policy indicates that HHS/CritiCall in its role as a prescribed person, does not routinely disclose PHI, unless permitted by *PHIPA* and its accompanying Regulation. This privacy policy and procedures imposes conditions and/or restrictions on the purposes for which and the circumstances in which an agent granted approval to access and use PHI is permitted to disclose that PHI. All employees, agents and vendors that are permitted to disclose PHI, may only do so under the direction of the CritiCall Privacy Lead, the CritiCall Executive Director and the Chief Privacy Officer, HHS. All disclosures of PHI shall be in compliance with *PHIPA* and its Regulation, *P12: Policy and Procedures for Disclosure of Personal Health Information for Purposes other than Research*; *P24: Policy and Procedures with Respect to De-Identification and Aggregation*; *P13: Policy and Procedures for Disclosures of Personal Health Information for Research and the Execution of Research Agreements.*

Notification and Termination of Access and Use

This privacy policy states that HHS/CritiCall shall permit access to PHI to authorized employees, agents and vendors so that they may fulfill their job-related duties. All employees, agents or vendors authorized to access the PHI in the CCIS must notify their supervisor/manager or HHS/CritiCall CCIS related contact in order to terminate their access privileges, if:

- They are no longer under contract with HHS/CritiCall;
- No longer operate as employees of the HHS/CritiCall for the CCIS; or
- No longer require access to the PHI in the CCIS.

This privacy policy requires that all supervisor/managers of employees, agents and vendors that are advised of a contract or employee termination (voluntary or involuntary), or that an employee, agent or vendor no longer requires access to the PHI in the CCIS, must notify the HHS Human Resources CritiCall Business Partner of the termination of the employment of HHS/CritiCall staff with access to CCIS. This privacy policy requires that notification be provided in advance of termination so that the HHS Human Resources CritiCall Business Partner may advise on the course of action to be taken. This privacy policy outlines the following requirements, with regard to providing notification:

- The documentation that must be completed, provided or executed;
- The agents responsible for the documentation
- The agents to whom the documentation must be provided; and

- The required content of the documentation.

This privacy policy also outlines the agents responsible for terminating access to and use of PHI, the procedure to be followed, and the time frame within which access to and use of PHI must be terminated.

The above procedures are aligned with and further discussed in *H10: Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship.*

Secure Retention and Destruction of Personal Health Information

This privacy policy indicates that all employees, agents and vendors granted access to use PHI within the CCIS must keep all PHI confidential and securely retain the information in compliance with *S5: Policy and Procedures for Secure Retention of Records of Personal Health Information*. In addition, all employees, agents and vendors granted access to use PHI within the CCIS shall, whenever required, securely dispose of all records of PHI in compliance with *S8: Policy and Procedures for Secure Disposal of Records of Personal Health Information.*

Tracking of Approved Access

This privacy policy requires the Manager, Information Technology or delegate to maintain a log of all persons that have been granted access to use PHI to perform their CCIS job-related duties. All approved/denied *CCIS Access to PHI Request Forms* along with the *P9: Access to PHI Log* shall be stored on the HHS/CritiCall document repository SharePoint.

Compliance, Audit and Enforcement

This privacy policy requires that all HHS/CritiCall employees and agents that support CCIS must comply with this policy. The CritiCall Privacy Lead is responsible for conducting an annual audit of this privacy policy and procedures and for ensuring compliance with this privacy policy and procedures. The annual audit will be conducted in accordance with *P27 Policy and Procedures in Respect of Privacy Audits.*

If a breach of this policy is found to have occurred an investigation will be conducted by the CritiCall Privacy Lead. This privacy policy and procedures indicates that if a breach, a suspected breach or a privacy risk with regards to the access or use of PHI is identified by an HHS/CritiCall employee, agent or vendor they must contact the CritiCall Privacy Lead at the first reasonable opportunity. The CritiCall Privacy Lead will initiate a privacy investigation. Each investigation will follow the steps outlined within *P29: Policy and Procedures for Privacy Breach Management*.

P9. LOG OF AGENTS GRANTED APPROVAL TO ACCESS AND USE PERSONAL HEALTH INFORMATION

HHS/CritiCall has implemented and maintains a log of agents who have been granted approval to access and use PHI, in accordance with *P8: Policy and Procedures for Limiting Agent Access to and*

Use of Personal Health Information. The "Log of Agents Granted Approval to Access and Use PHI" is maintained by the CCIS Project Manager under the direction of the CritiCall Privacy Lead. This privacy policy requires the following information to be included in the log:

- Name of the agent granted approval to access and use PHI;
- The data holdings of PHI to which the agent has been granted approval to access and use;
- The level or type of access and use granted;
- The date that access and use was granted; and
- The termination date or the date of the next audit of access to and use of PHI.

P10. POLICY AND PROCEDURES FOR THE USE OF PERSONAL HEALTH INFORMATION FOR RESEARCH

HHS/CritiCall has implemented a policy and procedures to identify the circumstances under which agents are permitted to use PHI for research.

This privacy policy prohibits the use of PHI for research if other information will serve the research purpose and states that no more PHI will be used than is reasonably necessary to meet the research purpose. This policy distinguishes between the use of PHI for research purposes and the use of PHI for purposes of section 39(1)(c) or section 45 of *PHIPA*, as the case may be.

The policy states that agents must comply with the policy and that compliance is audited on an ongoing basis by the Privacy Officer in accordance with policy *P27: Privacy Audits*. Where an agent is found to be non-compliant with the policy, HHS/CritiCall shall rely upon *H11: Discipline and Corrective Action.*

This policy requires agents to notify the CritiCall Privacy Lead at the first reasonable opportunity of a breach or suspect breach in accordance with policy *P29: Privacy Breach Management* and to notify the CritiCall Privacy Lead and the CritiCall Security Lead of a security breach or suspected breach as per policy *S17: Security Breach Management*.

Where the Use of Personal Health Information is Permitted for Research

This policy stipulates that HHS/CritiCall permits the use of PHI for research purposes as authorized under *PHIPA*, so long as:

- HHS/CritiCall agents meet the requirements for research as per *PHIPA* and the associated *Regulation*; and
- The purpose for the use of PHI is in accordance with the stated purpose for the Registry.

Distinction between the Use of Personal Health Information for Research and Other Purposes

This privacy policy indicates that while reviewing a request by an agent to use PHI, the CritiCall Privacy Lead shall confirm that the request constitutes a research use. This privacy policy and procedures clearly distinguishes between the use of PHI for research purposes and the use of PHI for

purposes of section 39(1)(c) or section 45 of the Act, as the case may be. This policy outlines the procedure to be adhered to in completing the review. A request is not research if the request:

- Does not test a specified hypothesis;
- Is intended to provide data for quality improvement or resource allocation analysis for health care; or
- It relates to improving the care for a specific individual.

Review and Approval Process

This privacy policy and procedures stipulates that agents may request the use of PHI or aggregated or de-identified data from CCIS for research by submitting a completed CCIS Data Request Form (For Research), a written research plan, and a copy of the decision of a research ethics board approving the research, to the CritiCall Privacy Lead. In addition, the policy requires the following particulars to be provided by the agent:

a) Name of the requesting agent;
b) Name and contact details of the Principal Investigator and their Role/Title within the organization;
c) Name of any Co-Investigator and their Role/Title within their organization;
d) Type of organization requesting the information;
e) The title of the study;
f) A description of the study;
g) Do the investigators plan on contacting any patients?
h) Research Ethics Board (REB) submission and status (approved/not approved/submitted);
i) Name of REB(s) and Name and contact information of the Chair of the REB;
j) Will the study be peer reviewed?
k) A list of the PHI (data elements) being requested or a list of the de-identified or aggregate data elements being requested;
l) If it is possible to conduct the research without the use of the PHI requested;
m) List of all investigators that will have access to the PHI, their title and affiliation with the study; why they require access to the PHI;
n) The safeguards that will be applied to the PHI (including physical, technical and administrative);
o) If the PHI or de-identified or aggregate data will be linked to other data? PHI from other sources?
p) The length of time the data is to be used by the organization;
q) Agreement that data will be destroyed/returned at the end of the approved period of use, in a secure manner prescribed by HHS/CritiCall;
r) Benefits/harms that could occur based on the study; and
s) If the request is for an extension on the use of PHI or de-identified or aggregate data previously disclosed by HHS/CritiCall to the requestor.

This policy requires the CritiCall Privacy Lead to review the request to use PHI for research purposes and confirm the criteria is met prior to approving or denying the request to use PHI for research purposes. This includes requiring the CritiCall Privacy Lead to review the written research plan to ensure it complies with the requirements in the *Act* and its Regulation; to ensure that the

written research plan has been approved by a research ethics board; and to ensure that HHS/CritiCall is in receipt of a copy of the decision of the research ethics board approving the written research plan. The policy considers *PHIPA* and the associated Regulation in determining the appropriate criteria. The CritiCall Privacy Lead shall also ensure that other information, namely de-identified and/or aggregate information, will not serve the research purpose and that no more PHI is being requested than is reasonably necessary to meet the research purpose.

The CritiCall Privacy Lead is responsible for submitting the reviewed requests to the CCIS Data Stewardship Committee for ultimate approval. The CCIS Data Stewardship Committee, at a minimum, must consider the following criteria:

a) Can the purpose of the requestor be satisfied with the release of aggregate or de-identified data?
b) Does the PHI being requested appear to be an over collection of PHI (is the minimum data set being requested in order to meet the needs of the study)?
c) Is the data being requested consistent with the data identified in the research plan?
d) Does the CCIS data being requested exist within the data holding and if yes, what is the integrity of the data?
e) Is the use aligned with the Critical Care Services Ontario and HHS/CritiCall mandates?
f) Does PHIPA permit the use?
g) What are the restrictions and conditions for the use, as noted in PHIPA and CCIS policy? and
h) Has enough detail been provided by the study to allow for a decision to be made at the time of review, or are additional details required form the requestor. If additional details are required, the CCIS Data Stewardship Committee secretary shall contact the Principal Investigator for more details. The request, with additional details will be further reviewed at the next CCIS Data Stewardship Committee meeting.

The policy stipulates that where the CCIS Data Stewardship Committee approves a request, the CritiCall Privacy Lead prepares a letter of approval and communicates this electronically to the agent making the request. The content of the approval letter is outlined in the policy.

Conditions or Restrictions on the Approval

As per this privacy policy and procedures, the following are conditions and restrictions that will be imposed on the approval to use PHI for research purposes, including any documentation that must be completed, provided or executed, which will be required of a requestor of PHI from HHS/CritiCall for the CCIS, prior to an approved use of PHI for research purposes. Pursuant to section 44(6) (a) to (g) of *PHIPA* a researcher who receives PHI about an individual from HHS/CritiCall shall,

(a) Comply with the conditions, if any, as specified by the research ethics board in respect of the research plan;
(b) Use the information only for the purposes set out in the research plan as approved by the research ethics board;

(c) Not publish the information in a form that could reasonably enable a person to ascertain the identity of an individual;
(d) Not disclose the information, except as required by law and subject to the exceptions and additional requirements, if any, that are prescribed;
(e) Not make contact or attempt to make contact with the individual, directly or indirectly, unless the custodian first obtains the individual's consent to being contacted;
(f) Notify the custodian immediately in writing if the researcher becomes aware of any breach of these conditions and restrictions; and
(g) Comply with the agreement described in subsection (5).

The CritiCall Privacy Lead is responsible for completing, providing or executing the documentation and for ensuring that any conditions or restrictions imposed on the use of PHI for research purposes are in fact satisfied.

Secure Retention

This privacy policy states that the agent, who is granted approval to use PHI for research purposes, shall retain the records of PHI in compliance with the written research plan approved by the research ethics board and in compliance with the *S5: Policy and Procedures for Secure Retention of Records of Personal Health Information.*

Secure Return or Disposal

This privacy policy requires that each approved use of PHI by the CCIS Data Stewardship Committee include a period, or term, for which the researchers may access and use the PHI from the CCIS. This privacy policy and procedures states that the written research plan must include the time frame following the retention period within which the records must be securely disposed of, requires a certificate of destruction be provided, and identifies the CritiCall Privacy Lead as being responsible for receiving the certificate of destruction and identifies the time frame following secure disposal within which the certificate of disposal must be provided. Once the term has elapsed, the CritiCall Privacy Lead shall contact the requesting agent, to arrange for the:

a) The secure destruction of the PHI received from the CCIS which must be in compliance with *S8: CCIS Policy and Procedure for the Secure Disposal of Records of Personal Health Information*; or
b) Submission of another CCIS Request for Data Form for extension of the term for access/use of PHI from the CCIS.

This privacy policy and procedures identifies the CritiCall Privacy Lead as the responsible person for ensuring records of PHI used for research purposes are securely returned, securely disposed of or de-identified within the stipulated time frame following the retention period set out in the written research plan and the process to be followed in the event that the records of PHI are not securely returned, a certificate of destruction is not received or the records of PHI are not de-identified within the time frame identified.

Where a certificate of destruction is not received within one month following the period or term where permission to access and use the PHI has elapsed, the CritiCall Privacy Lead will escalate the issue to the Executive Director, CritiCall. The Executive Director, CritiCall shall contact the agent

who received the PHI from the CCIS to arrange for the secure destruction of the PHI. The Executive Director, CritiCall shall escalate this issue to General Counsel at HHS, as required.

As per this privacy policy, the certificate of destruction must identify the records of PHI securely disposed of and the date, time and method of secure disposal employed and that the certificate must bear the name and signature of the agent who performed the secure disposal.

Tracking Approved Uses of Personal Health Information for Research

This privacy policy and procedures requires that a log be maintained of the approved uses of personal health information for research purposes and must identify the agent(s) responsible for maintaining such a log. This privacy policy and procedures also addresses where written research plans, copies of the decisions of research ethics boards, certificates of destruction and other documentation related to the receipt, review, approval or denial of requests for the use of personal health information for research purposes will be retained and the agent(s) responsible for retaining this documentation.

Where the Use of PHI is not Permitted for Research

If HHS/CritiCall determines that the request for PHI for research purposes is not approved, the CCIS Data Stewardship Committee may review the request for data and determine whether de-identified or aggregate data may be disclosed for research purposes.

Review and Approval Process

This policy and procedures identifies the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the use of de- identified and/or aggregate information for research purposes and the process that must be followed in this regard. This policy and procedures includes a discussion of the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

This policy and procedures also addresses the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request to use de-identified and/or aggregate information for research purposes. This policy and procedures requires the de-identified and/or aggregate information to be reviewed prior to the approval and use of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and 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. The agent(s) responsible for undertaking this review is identified.

This policy and procedures also sets out the manner in which the decision approving or denying the request for the use of de-identified and/or aggregate information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

Conditions or Restrictions on the Approval

This policy and procedures identifies the conditions and/or restrictions that will be imposed on the approval to use de-identified and/or aggregate information for research purposes, including any documentation that must be completed, provided or executed and the agent(s) responsible for completing, providing or executing the documentation.

This policy and procedures prohibits an agent granted approval to use de- identified and/or aggregate information for research purposes from using that information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

This policy and procedures identifies the agent(s) responsible for ensuring that any conditions or restrictions imposed on the use of de-identified and/or aggregate information for research purposes are in fact being satisfied.

P11. LOG OF APPROVED USES OF PERSONAL HEALTH INFORMATION FOR RESEARCH

HHS/CritiCall has implemented and maintains a log of approved uses of PHI for research. The log is maintained and updated by the CritiCall Privacy Lead. The log includes the following information:

- The name of the research study;
- The name of the agent(s) to whom the approval was granted;
- The date of the decision of the research ethics board approving the written research plan;
- The date that the approval to use PHI for research purposes was granted by the prescribed person or prescribed entity;
- The date that the PHI was provided to the agent(s);
- The nature of the PHI provided to the agent(s);
- The retention period for the records of PHI identified in the written research plan approved by the research ethics board;
- Whether the records of PHI will be securely returned, securely disposed of or de-identified and retained following the retention period; and
- The date the records of PHI were securely returned or a certificate of destruction was received or the date by which they must be returned or disposed of, if applicable.

P12. POLICY AND PROCEDURES FOR DISCLOSURE OF PERSONAL HEALTH INFORMATION FOR PURPOSES OTHER THAN RESEARCH

HHS/CritiCall has developed and implemented a policy and procedures for the disclosure of PHI for purposes other than research. This policy and procedures outlines how HHS/CritiCall employees and other agents of HHS/CritiCall shall identify whether and under what circumstances PHI is permitted to be disclosed from the CCIS for any purpose other than research. This privacy policy requires that all HHS/CritiCall employees and agents comply with this policy and its procedures. The policy identifies that the CritiCall Privacy Lead is responsible for ensuring compliance is enforced and

outlines the consequences of a breach of this policy. This privacy policy and procedures stipulates that compliance will be audited by the CritiCall Privacy Lead in accordance with HHS/CritiCall's *Policy and Procedures in Respect of Privacy Audits* on an annual basis and the CritiCall Privacy Lead is responsible for ensuring compliance with this privacy policy and procedures.

HHS/CritiCall's privacy policy includes a commitment by the organization to not disclose PHI if other information will serve the purposes and that HHS/CritiCall will not disclose more information than is reasonably necessary to meet the purpose.

This privacy policy and procedures requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with *P-27: Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

Where the Disclosure of PHI is Permitted

HHS/CritiCall is permitted to disclose PHI from the CCIS to another prescribed person, a prescribed entity, a Medical Officer of Health, or a health data institute. This privacy policy and procedures requires that all disclosures of PHI comply with the Act and its Regulation. In addition, this privacy policy and procedures sets out the purposes for which and the circumstances in which the disclosure of PHI is permitted.

Any requests made to HHS/CritiCall with regards to PHI held in the CCIS which require a disclosure by law, fall outside of the scope of these procedures. Requests where disclosures are required by law (e.g. law enforcement request) shall be directed to and managed by the Executive Director, CritiCall, the Executive Vice President and Chief Operating Officer and if required, the HHS Chief Privacy Officer.

Review and Approval Process

This privacy policy indicates that the CritiCall Privacy Lead is responsible for reviewing the disclosure of PHI request. If the CritiCall Privacy Lead establishes that the disclosure is permitted under *PHIPA*, the CritiCall Privacy Lead will document his/her comments/opinions on the *CCIS Data Request Form (Not for Research)* and add the new request to the agenda of the CCIS Data Stewardship Committee.

This privacy policy requires the requesting party to complete a *CCIS Data Request Form (Not for Research)* found on the HHS/CritiCall website (this is the only documentation required from the requestor). The form must be completed in full by the requestor and include the following information: name of the requesting organization; name and contact details of the requestor; their role/title within the organization; type of organization requesting the information; If the request is being made by an internal requestor at HHS/CritiCall; if PHI being requested; if yes, a list of the PHI being requested; the purpose for the disclosure; if a PIA or privacy risk analysis has been completed on the request; the length of time the data is to be used by the requestor/organization; and if the request is for an extension on the use of PHI previously disclosed by HHS/CritiCall to the requestor. Once the form has been completed it must be signed by the requestor and forwarded to the CritiCall Privacy Lead.

This privacy policy indicates that the CCIS Data Stewardship Committee shall review all new requests at each meeting to determine if a disclosure of PHI will be approved. Among other

considerations, the policy indicates that the CCIS Data Stewardship Committee shall at a minimum consider the following criteria:

- The agent responsible for determining whether to approve or deny the request to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose of the disclosure and that no more PHI is being requested than is reasonably necessary to meet the identified purpose.
- Does the PHI being requested appear to be an over collection of PHI (is the minimum data set being requested in order to meet the needs of the requestor)?
- Does the CCIS data being requested, exist within the data holding and if yes, what is the integrity of the data?
- Is the disclosure aligned with the CCSO and HHS/CritiCall mandate?
- Does PHIPA permit the disclosure?
- What are the restrictions and conditions for the disclosure, as noted in PHIPA and CCIS policies?
- Has enough detail been provided by the requestor to allow for a decision to be made at the time of review, or are additional details required from the requestor? If additional details are required, the CCIS Data Stewardship Committee secretary shall contact the requestor for more details. The request, with additional details will be further reviewed at the next CCIS Data Stewardship Committee meeting.

This privacy policy states that if sufficient details have been provided by the requestor and the request is approved by the CCIS Data Stewardship Committee, the CritiCall Privacy Lead shall log the approval, ascertain sign-off by the committee Chair(s) – on the *CCIS Data Request Form (Not for Research)* - and record any conditions that must be satisfied, before the disclosure is made.

This privacy policy indicates that if the CCIS Data Stewardship Committee determines that the request shall not be approved, the CritiCall Privacy Lead shall log the not-approved status of the request and ascertain sign-off by the committee Chair(s) on the *CCIS Data Request Form (Not for Research)*.

This privacy policy states that a letter signed by the CCIS Data Stewardship Committee chairs will be sent by the CritiCall Privacy Lead via email to the requestor advising them of the decision to release/not release the PHI to their organization. If the request has been approved, the letter will list the conditions which must be satisfied prior to the transfer of PHI. The CritiCall Privacy Lead will be noted as the primary contact for addressing and confirming that all conditions and restrictions are met.

This privacy policy states that the CritiCall Privacy Lead will advise the CCIS Product Manager once all conditions and restrictions have been satisfied. The PHI for disclosure may then be prepared for release.

This privacy policy requires that the CritiCall Privacy Lead shall log the date when all conditions and restrictions were satisfied.

This privacy policy states that once all conditions and restrictions have been satisfied, the CCIS Product Manager shall arrange for the CCIS Decision Support Staff to retrieve the required data set for disclosure, in the format requested.

This privacy policy states that the CCIS Product Manager will review the data set prepared by CCIS Decision Support Staff to ensure that it is limited to only that PHI that has been requested/approved for release.

Conditions or Restrictions on the Approval

This privacy policy outlines the following conditions and restrictions and indicates that the CritiCall Privacy Lead is responsible for ensuring that any conditions or restrictions are satisfied prior to the disclosure of the PHI for purposes other than research. This privacy policy and procedures states that if a disclosure of PHI is approved by the CCIS Data Stewardship Committee, the CritiCall Privacy Lead is responsible for completing, providing and/or executing the documentation and/or agreements that must be completed, provided or executed. This privacy policy and procedure outlines the documentation that is required. A data sharing agreement is executed with the requesting organization. The following are conditions and restrictions, as per this privacy policy, required of a requestor, prior to an approved disclosure of PHI for purposes other than research:

1. PHIPA Restrictions:
   The CritiCall Privacy Lead shall determine if there are any restrictions imposed by *PHIPA* and its accompanying Regulation on the disclosure of PHI to the requesting party. If any restrictions or conditions exist under *PHIPA*, the CritiCall Privacy Lead shall identify these during preliminary review of the request and document the restrictions and conditions in the *CCIS Data Request Form (Not for Research)*. If the request for disclosure does not comply with any restrictions or conditions set out in PHIPA, a PHI disclosure to an approved requesting organization shall not be made.

2. Execution of Data Sharing Agreements (for PHI):
   This privacy policy and procedure states that if a disclosure of PHI is approved by the CCIS Data Stewardship Committee, the CritiCall Privacy Lead is responsible for ensuring that a data sharing agreement is executed with the requesting organization. Each Data Sharing Agreement (for PHI) outlines the legal authority for the disclosure, the terms of the release and the minimum privacy/security standards which must be applied to the PHI received by the requesting organization. A data disclosure to an approved organization shall not be made without an executed Data Sharing Agreement (for PHI), as per *P17: Template Data Sharing Agreement*. Each Data Sharing Agreement (for PHI) will be processed in compliance with *P16: CCIS Policy and Procedures for the Execution of Data Sharing Agreement*.

3. Transfer of PHI:
   HHS/CritiCall and the requesting organization, must agree to a secure means for the transport of PHI, which is in compliance with *S7: CCIS Policy and Procedures for Secure Transfer for Records of Personal Health Information.* The means of transfer shall be identified for both sending the PHI to the approved organization and the return of that PHI.

4. Period of Use for the PHI, Secure Return or Disposal:
   Each approved disclosure of PHI by the CCIS Data Stewardship Committee shall include a period, or term, for which the requesting organization may access and use the PHI from the CCIS. Once the term has elapsed, CritiCall Privacy Lead shall contact the requesting organization, to arrange for the secure return of the PHI, or secure destruction and a certificate of destruction.

Secure Transfer

This privacy policy states that HHS/CritiCall and the requesting organization, must agree to a secure means for the transport of PHI which is in compliance with *S7: CCIS Policy and Procedures for Secure Transfer for Records of Personal Health Information*. The means of transfer shall be identified for both sending the PHI to the approved organization and the return of that PHI.

Secure Return or Disposal

This privacy policy requires that each approved disclosure of PHI by the CCIS Data Stewardship Committee shall include a period, or term, for which the requesting organization may access and use the PHI from the CCIS, as set out in the Data Sharing Agreement. This privacy policy indicates that once the term has elapsed, CritiCall Privacy Lead shall contact the requesting organization, to arrange for the:

- Secure return of the PHI received from the CCIS which must be in compliance with *S7 – CCIS Policy and Procedures for Secure Transfer for Records of Personal Health Information;* or
- secure destruction and a certificate of destruction of the PHI received from the CCIS which must be in compliance with *S8: CCIS Policy and Procedures for the Secure Disposal of Records of Personal Health Information*; or
- Submission of another *CCIS Request for Data Form* for extension of the term for access/use of PHI from the CCIS.

This privacy policy states that where records of PHI are not securely returned or a certificate of destruction is not received within one month following the period or term where permission to access and use the PHI has elapsed, the CritiCall Privacy Lead will escalate the issue to the CritiCall Executive Director. The CritiCall, Executive Director shall contact the organization that received the PHI from the CCIS to arrange for return or destruction of the PHI. The Executive Director, CritiCall shall escalate this issue to General Counsel at HHS, as required.

Documentation Related to Approved Disclosures of Personal Health Information

This privacy policy states that all documentation related to each PHI disclosure shall be maintained by the CritiCall Privacy Lead on a secure location within the HHS/CritiCall SharePoint. The documentation includes completed approved or not approved CCIS Data Request Forms; any CritiCall Privacy Lead comments/conditions/restriction; approval forms signed by the CCIS Data Stewardship Committee Chair; logs/Meeting Notes; logs and list of data elements released by the CCIS Product Manager.

B. WHERE THE DISCLOSURE OF PHI IS NOT PERMITTED

This privacy policy and procedures requires that all aggregate reporting is reviewed prior to its disclosure in order to ensure that there is no PHI included and that data is aggregated or de-identified in accordance with the *P24: CCIS Policy and Procedures with Respect to De-Identification and Aggregation.*

Review and Approval Process

This privacy policy states that the CritiCall Privacy Lead is responsible for receiving, reviewing and determining whether a request for disclosure of de-identified and/or aggregate data is approved or denied. When any person requests a disclosure of de-identified and/or aggregate data from the CCIS for non-research purposes, numerous steps are to be followed. The requesting party must complete a *CCIS Data Request Form (Not for Research)* found on the CritiCall website. The form requires the following information from the requestor:

- Name of the requesting organization;
- Name and contact details of the requestor;
- Their role/title within the organization;
- Type of organization requesting the information;
- If the request is being made by an internal requestor at HHS/CritiCall;
- The purpose for the disclosure;
- If a Privacy Impact Assessment (PIA) or privacy risk analysis has been completed on the request;
- The length of time the data is to be used by the organization; and
- If the request is for an extension on the use of PHI previously disclosed by HHS/CritiCall to the requestor.

This privacy policy requires that once the form has been completed it must be signed by the requestor and forwarded to the CritiCall Privacy Lead. The CritiCall Privacy Lead shall review the request to ensure the appropriate forms are completed; determine whether there are any conditions or restrictions applicable to accessing the de-identified and/or aggregate data; and determine a secure means of transferring the requested data. The CritiCall Privacy Lead will maintain a copy of all documentation related to the request which shall be maintained on a secure location within the HHS/CritiCall SharePoint including:

- Completed approved or not approved *CCIS Data Request Forms*; and
- CritiCall Privacy Lead comments and decision to transfer the request to the CCIS Data Stewardship Committee

The CCIS Data Stewardship Committee is responsible for reviewing all new requests and determine if a disclosure of de-identified or aggregate data will be approved. Among other considerations, the committee shall, at a minimum, consider the following criteria:

- Does the aggregate or de-identified data being requested exist within the data holding and if yes, what is the integrity of the data?
- Is the data aggregated or de-identified in compliance with *P24: CCIS Policy and Procedures with Respect to De-Identification and Aggregation*, so that it cannot be easily re-engineered to identify an individual?
- Is the release of aggregate or de-identified data aligned with the HHS/CritiCall mandate?
- What are the restrictions and conditions for the release of data, as noted by the CritiCall Privacy Lead?; and
- Has enough detail been provided by the requestor to allow for a decision to be made at the time of review, or are additional details required form the requestor? If additional details are

required, the CCIS Data Stewardship Committee secretary shall contact the requestor for more details. The request, with additional details will be further reviewed at the next CCIS Data Stewardship Committee meeting.

This privacy policy indicates that if the request is approved by the CCIS Data Stewardship Committee, then the CCIS Data Stewardship Committee secretary shall log the approval, ascertain sign-off by the committee Chair(s) – on the *CCIS Data Request Form (Not for Research)* - and record any conditions that must be satisfied, before the data is released. If the CCIS Data Stewardship Committee determines that the request shall not be approved, the CCIS Data Stewardship Committee secretary shall log the not-approved status of the request and ascertain sign-off by the committee Chair(s) on the *CCIS Data Request Form (for Research)*.

This privacy policy indicates that the requestor will be notified of the CCIS Data Stewardship Committee's decision to release/not release the aggregate or de-identified data to their organization by way of letter. If the request was approved, the letter outlines any and all conditions which must first be satisfied prior to the transfer of de-identified and/or aggregate data. The CritiCall Privacy lead will be noted as the primary contact person. The CritiCall Privacy Lead shall log the date when all conditions and restrictions were satisfied. Once all conditions are satisfied, the CCIS Product Manager shall review the data set to ensure it is limited to only the approved aggregate or de-identified data.

This privacy policy indicates that the CCIS Product Manager will then transfer the de-identified and/or aggregate dataset to the requesting organization, in compliance with *S7: CCIS Policy and Procedures for Secure Transfer for Records of Personal Health Information*.

This privacy policy requires that the CCIS Product Manager must keep a log of the data release and the date of transmission. All documentation related to each de-identified and/or aggregate data disclosure shall be maintained on a secure location within the HHS/CritiCall SharePoint.

Conditions or Restrictions on the Approval

The CritiCall Privacy Lead is responsible for ensuring that any conditions or restrictions that must be satisfied before the disclosure of de-identified and/or aggregate data are met. The following are conditions and restrictions that are required to be satisfied prior to the disclosure of de-identified and/or aggregate data will be required of a requestor of aggregate or de-identified data from HHS/CritiCall for the CCIS, prior to an approved release of data for purposes other than research.

1. **Execution of Data Sharing Agreement (for the Release of Aggregate or De-identified Data):**
   Each Data Sharing Agreement (for the Release of Aggregate or De-identified Data) outlines the terms for the release for the aggregate or de-identified data received by the requesting organization. Each Data Sharing Agreement (for the Release of Aggregate or De-identified Data) must stipulate that the person who received aggregate/de-identified data from the CCIS will not use that data either alone or with other information, to attempt to identify an

individual. This includes attempting to decrypt information that is encrypted in an attempt to identify an individual based with prior knowledge of that individual.

A release of aggregate or de-identified data to an approved organization shall not be made without an executed Data Sharing Agreement (for the Release of Aggregate or De-identified Data).

2. **Transfer of** De-identified and/or Aggregate Data**:**
HHS/CritiCall and the requesting organization, must agree to a secure means for the transport of any aggregate or de-identified data in compliance with *S7: CCIS Policy and Procedures for Secure Transfer for Records of Personal Health Information*.

The policy and procedures identifies that the CritiCall Privacy Lead is responsible for ensuring that any conditions or restrictions have been satisfied prior to the disclosure of the de-identified and/or aggregate information, including the execution of the written acknowledgement. The CritiCall Privacy Lead is also responsible for tracking the receipt of the executed written acknowledgments and documenting the information in the Log of Data Sharing Agreements.

P13. POLICY AND PROCEDURES FOR DISCLOSURE OF PERSONAL HEALTH INFORMATION FOR RESEARCH PURPOSES AND THE EXECUTION OF RESEARCH AGREEMENTS

HHS/CritiCall has developed and implemented a policy and procedures for the disclosure of PHI for research purposes and the execution of research agreements. This privacy policy and procedures requires all HHS/CritiCall agents to comply with this policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of a breach. Compliance will be audited in accordance with P-*28 Policy and Procedures in Respect of Privacy Audits* on an annual basis at the direction of the CritiCall Privacy Lead, who is also responsible for ensuring compliance with this privacy policy and procedures.

This policy and procedures outlines how HHS/CritiCall employees and any other agents of HHS, with respect to its role as a prescribed person, shall identify whether and under what circumstances PHI in CCIS is permitted to be disclosed by HHS/CritiCall for research purposes. In identifying whether and under what circumstances PHI may be released for research purposes, HHS/CritiCall's policy and procedures articulates a commitment not to disclose PHI for research purposes if other information will serve the research purpose and not to disclose more PHI than is reasonably necessary to meet the research purpose.

This privacy policy and procedures requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with *CCIS P-30 Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

Review and Approval Process

This privacy policy states that HHS/CritiCall will disclose PHI from the CCIS to researchers that conduct research studies if the researchers have fulfilled their obligations under section 44 of *PHIPA*

and are subsequently approved by the CCIS Data Stewardship Committee, as outlined in the procedures below.

This privacy policy and procedures requires the CritiCall Privacy Lead, who is responsible for determining whether to approve or deny the request, to ensure that HHS/CritiCall is in receipt of a written application, a written research plan, and a copy of the decision of the research ethics board approving the written research plan and that the written research plan complies with the requirements in the *Act* and its regulation.

This privacy policy indicates that the CritiCall Privacy Lead is responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of PHI for research purposes. This privacy policy outlines the documentation that must be completed, provided and executed by the agents, to whom it must be provided, and the content of the required documentation. A requestor must complete a *CCIS Data Request Form (For Research)* and forward the completed form to the CritiCall Privacy Lead. The *CCIS Data Request Form (For Research)* is found on the CritiCall website. The form must be completed in full and include the following details:

- Name of the requesting organization;
- Name and contact details of the Principal Investigator and their Role/Title within the organization;
- Name of any Co-Investigator and their Role/Title within their organization;
- Type of organization requesting the information;
- The title of the study;
- A description of the study;
- Whether the investigators plan on contacting any patients?
- Research Ethics Board (REB) submission and status (approved/not approved/submitted);
- Name of REB(s) and Name and contact information of the Chair of the REB;
- Whether the study be peer reviewed?
- A list of the PHI (data elements) being requested or a list of the de-identified or aggregate data elements being requested;
- If it is possible to conduct the research without the use of the PHI requested;
- List of all investigators that will have access to the PHI, their title and affiliation with the study; and why they require access to the PHI;
- The safeguards that will be applied to the PHI (including physical, technical and administrative);
- If the PHI or de-identified or aggregate data will be linked to other data? e.g. PHI from other sources?
- The length of time the data is to be used by the organization;
- Agreement that data will be destroyed/returned at the end of the approved period of use, in a secure manner prescribed by HHS/CritiCall;
- Benefits/harms that could occur based on the study; and
- If the request is for an extension on the use of PHI or de-identified or aggregate data previously disclosed by HHS/CritiCall to the requestor.

This privacy policy and procedures states that upon receipt of the *CCIS Data Request Form (For Research)*, the CritiCall Privacy Lead is responsible to review and confirm that the request meets the following requirements:

- If the study plans on directly contacting patients and any restrictions imposed by *PHIPA* on this matter;
- The existence of any scripts/communications to be sent to patients, as approved by the REB;
- If *PHIPA* permits the disclosure from HHS/CritiCall as a prescribed person, to the study;
- If any conditions or restriction are noted with *PHIPA* prior to the disclosure (i.e. are all of the terms of section 44 of *PHIPA* fulfilled?); or
- Secure means of transport and the format of PHI requested (i.e. paper, electronic).

If the CritiCall Privacy Lead establishes that the disclosure is permitted under *PHIPA* the CritiCall Privacy Lead will document his/her comments/opinion on the *CCIS Data Request Form (for Research)* and add the new request to the agenda for the CCIS Data Stewardship Committee meeting. The CCIS Data Stewardship Committee must review all requests for PHI and de-identified or aggregate data from the CCIS for research and determine whether the request will be approved.

- Among other considerations the committee shall at a minimum consider the following criteria:

    a. Can the purpose of the requestor be satisfied with the release of aggregate or de-identified data?
    b. Does the PHI being requested appear to be an over collection of PHI (is the minimum data being requested in order to meet the needs of the study)?
    c. Is the data being requested consistent with the data identified in the research plan?
    d. Does the CCIS data being requested exist within the data holding and if yes, what is the integrity of the data?
    e. Is the disclosure aligned with the CCSO and HHS/CritiCall mandates?
    f. Does PHIPA permit the disclosure?
    g. What are the restrictions and conditions for the disclosure, as noted in *PHIPA* and the CCIS policy?
    h. Has enough detail been provided about the research to allow for a decision to be made at the time of review, or are additional details required from the requestor. If additional details are required, the Privacy Lead shall contact the Principal Investigator for more details. The request, with additional details will be further reviewed at the next CCIS Data Stewardship Committee meeting.

This privacy policy states that if sufficient details have been provided and the request is approved by the CCIS Data Stewardship Committee, the CritiCall Privacy Lead shall log the approval, ascertain sign-off by the committee Chair(s) – on the *CCIS Data Request Form (for Research)* and record any conditions that must be satisfied, before the disclosure is made.

This privacy policy requires that if the CCIS Data Stewardship Committee determines that the research shall not be supported with PHI from the CCIS, the CritiCall Privacy Lead shall log the not-approved status of the request and ascertain sign-off by the committee Chair(s) on the *CCIS Data Request Form (for Research)*.

This privacy policy states that a letter will be sent to the Principal Investigator advising of the decision to release/not release the PHI or de-identified or aggregate data for their research study and the reason for the decision. If the study has been approved, the letter will list the conditions that must be satisfied prior to the transfer of PHI, including an agreement respecting disclosure as required by section 44(5) of *PHIPA*. The CritiCall Privacy Lead will be the primary contact for addressing and confirming that all conditions and restrictions are met.

This privacy policy states that the CritiCall Privacy Lead will forward a copy of the Research Plan, REB approval and the letter of decision from the CCIS Data Stewardship Committee to the HHS Office of Research Administration. The HHS Office of Research Administration will prepare a draft of the Research Agreement for review by the Principal Investigator. During the review of the policy and procedures for disclosure of PHI for research in June 2019, it was noted that revisions were required as the procedures incorrectly referenced the involvement of the HHS Research Administration disclosure. The policy is currently under review as at this time the preparation and execution of the Research Agreement with the Principal Investigator is facilitated through the CritiCall Privacy Lead.

This privacy policy requires that once the Research Agreement is finalized and signed by the Principal Investigator, the CritiCall Privacy Lead will advise the CCIS Product Manager that all conditions and restrictions have been satisfied and the disclosure may then proceed.

The privacy policy requires that all documentation related to each disclosure, including written applications, written research plans, copies of the decisions of research ethics board, Research Agreements, certificates of destruction and other documentation related to the receipt, review, approval or denial of requests for the disclosure of personal health information for research purposes, shall be maintained on a secure location with the HHS/CritiCall document repository by the CritiCall Privacy Lead.

Conditions or Restrictions on the Approval of PHI Data for Research Purposes

This privacy policy outlines the following conditions and restrictions, which must be satisfied by a requestor of PHI from the CCIS, prior to an approved disclosure of PHI for the purposes of research. This privacy policy identifies the CritiCall Privacy Lead as being the responsible party for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of PHI have been satisfied.

1. <u>PHIPA Restrictions:</u>

This privacy policy states that if any restrictions or conditions exist under *PHIPA*, the CritiCall Privacy Lead shall identify these during their preliminary review of the request and document the restrictions and conditions in the *CCIS Data Request Form*. If the request for disclosure does not comply with any restrictions or conditions set out in *PHIPA*, a PHI disclosure to an approved requesting organization shall not be made.

2. <u>Execution of Research Agreements:</u>

This privacy policy states that if a disclosure of PHI is approved by the CCIS Data Stewardship Committee, a Research Agreement shall be executed with the researcher. A PHI disclosure to an

approved research study shall not be made without an executed Research Agreement. Each Research Agreement will carry the provisions outlined within *P14: CCIS Template Research Agreements.*

3. The privacy policy requires the submission of a written research plan in accordance with the Act and its regulation and requires research ethics board approval of the written research plan prior to the disclosure of de-identified and/or aggregate information for research purposes. Transfer of PHI:

This privacy policy states that HHS/CritiCall and the Principal Investigator must agree to a secure means for the transport of PHI which is in compliance with *S7: CCIS Policy and Procedures for Secure Transfer for Records of Personal Health Information*.

4. Period of Use for the PHI, Secure Disposal:

This privacy policy states that each approved disclosure of PHI by the CCIS Data Stewardship Committee shall include a period, or term, for which the researchers may access and use the PHI from the CCIS. Once the term has elapsed, the CritiCall Privacy Lead shall contact the requesting organization, to arrange for the:

- Secure destruction of the PHI received from the CCIS which must be in compliance with *S8: CCIS Policy and Procedures for the Secure Disposal of Records of Personal Health Information*; or
- Submission of another *CCIS Data Form* (for Research) for extension of the term for use of PHI from the CCIS for research.

Secure Transfer

This privacy policy and procedures requires the records of PHI which are disclosed for research purposes to be transferred in a secure manner in compliance with the *S-7 Policy and Procedures for Secure Transfer of Records of Personal Health Information.*

Secure Disposal

This privacy policy and procedures identifies that the CritiCall Privacy Lead is responsible for ensuring that records of PHI disclosed to a researcher for research purposes are securely disposed of or de-identified, as the case may be, following the retention period set out in the Research Agreement. This privacy policy and procedures further addresses the process to be followed by the CritiCall Privacy Lead where a certificate of destruction is not received or written confirmation of de-identification is not received for records of PHI within the time set out in the Research Agreement.

Where the Disclosure of Personal Health Information is not permitted for Research

This privacy policy and procedures states that PHI may be disclosed for research purposes in certain circumstances. If the disclosure of PHI is not permitted for research purposes, this privacy policy may permit de-identified and aggregate information to be disclosed for research purposes. The circumstances in which de-identified and aggregate information may be disclosed for research purposes is outlined below

Review and Approval Process

This privacy policy identifies that the CritiCall Privacy Lead is responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of de-identified and aggregate information for research purposes, as well as the process that must be followed in this regard. This privacy policy identifies the following particulars:

- The documentation that must be completed, provided and/or executed by agents of HHS/CritiCall;
- The documentation must be provided to the CritiCall Privacy Lead; and
- The required content of the documentation.

At a minimum, this privacy policy requires de-identified and/or aggregate information to be reviewed prior to the approval and disclosure of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and 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.

This privacy policy sets out the manner in which the decision approving or denying the request for the disclosure of de-identified and/or aggregate information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

Conditions or Restrictions on the Approval of Aggregate or De-Identified Information

This privacy policy states that the following conditions and restrictions, which may be required of a requestor of aggregate or de-identified data from HHS/CritiCall for the CCIS, must be satisfied prior to an approved release of aggregate or de-identified information for research purposes. The CritiCall Privacy Lead is responsible for ensuring all conditions and/or restrictions have been satisfied prior to the disclosure of the de-identified and aggregate information.

This privacy policy requires the researcher to whom the de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that the researcher will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge.

This policy also states that the CritiCall Privacy Lead is responsible for ensuring that any conditions or restrictions are satisfied prior to the disclosure of the de-identified and/or aggregate information have in fact been satisfied, including the execution of the written acknowledgement. Further, the policy and procedures requires the CritiCall Privacy Lead to track receipt of the executed written acknowledgments and sets out the procedure that must be followed and the documentation that must be maintained in this regard.

Conditions and Restrictions

1. Execution of Data Sharing Agreement (for the Release of Aggregate or De-identified Data):

If a release of aggregate or de-identified data is approved by the CCIS Data Stewardship Committee, a data sharing acknowledgement shall be executed in the form of a data sharing agreement with the requesting organization. Each data sharing agreement (for the disclosure of Aggregate or De-identified Data) outlines the terms for the disclosure of the aggregate or de-identified data received by the requesting organization.

2. Transfer of Aggregate or De-identified Data:

HHS/CritiCall and the requesting organization, must agree to a secure means for the transfer of any aggregate or de-identified data in compliance with *S7: CCIS Policy and Procedures for Secure Transfer for Records of Personal Health Information* as if it were *PHI*.

Compliance

This privacy policy requires that all HHS/CritiCall employees and agents comply with this policy and procedures. This policy and procedures shall be enforced by the CritiCall Privacy Lead to ensure that all requests for PHI from the CCIS that are related to research operate in compliance with the provisions of this policy.

This privacy policy indicates that the HHS Chief Privacy Officer, or delegate and the CritiCall Privacy Lead will conduct an annual audit of this policy and procedure in compliance with *P27: Policy and Procedures In Respect of Privacy Audits*. 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 Chief Privacy Officer. The HHS Chief Privacy Officer or delegate may conduct additional random audits at any time. The audit criteria and reporting requirements are further outlined within the *P27: Policy and Procedures In Respect of Privacy Audits.*

This privacy policy states that if a breach of this policy is found to have occurred, an investigation will be conducted by the CritiCall Privacy Lead. If a breach, a suspected breach or a privacy risk with regards to disclosure of PHI, related to research is identified, agents must contact the CCIS Help Desk at the first reasonable opportunity in accordance with *P29: Policy and Procedures for Privacy Breach Management*. 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 Procedures for Privacy Breach Management*.

P14. TEMPLATE RESEARCH AGREEMENT

HHS/CritiCall has developed and implemented a template Research Agreement that is executed with researchers to whom PHI will be disclosed prior to the disclosure of PHI for research purposes. The Research Agreement addresses the criteria documented below.

General Provisions

This privacy policy requires the Research Agreement to identify HHS/CritiCall as a "prescribed person" as defined in *PHIPA* and its regulation and the duties and responsibilities arising from this status. The Research Agreement outlines the legislative authority for the disclosure and the collection of the PHI under *PHIPA* and its regulation along with the terms for the collection, use, disclosure, retention/destruction and safeguards applied to the PHI. This includes the definition of PHI found in *PHIPA* and specifies the nature of the PHI that will be disclosed.

If a request for disclosure of PHI for research purposes is approved, the CritiCall Privacy Lead shall ensure that a Research Agreement is executed with the researchers to whom the PHI is to be disclosed.

Purposes of Collection, Use and Disclosure

This privacy policy states that the research purpose for which the PHI is being disclosed by HHS/CritiCall and the purposes for which the PHI may be used or disclosed by the researcher must be identified in the Research Agreement in addition to the statutory authority for each collection, use and disclosure identified.

This privacy policy indicates that the Research Agreement permits the researcher to only use the PHI for purposes set out in the written research plan approved by the research ethics board and prohibits the use of the PHI for any other purpose. The Research Agreement prohibits the researcher from permitting persons to access and use the PHI except those persons described in the written research plan approved by the research ethics board.

The Research Agreement explicitly states whether or not the PHI may be linked to other information and prohibits the PHI from being linked except in accordance with the written research plan approved by the research ethics board.

This privacy policy states that the Research Agreement must include the following:

- The researcher must acknowledge that the PHI being disclosed pursuant to the Research Agreement is necessary for the identified research purposes and that other information such as de-identified and/or aggregate information, will not serve the research purposes;
- The researcher must acknowledge that no more PHI is being disclosed and will be collected and used than is reasonably necessary to meet the research purpose;
- The researcher must acknowledge and agree not to disclose the PHI except as required by law and subject to the exceptions and additional requirements prescribed by *PHIPA*;
- The researcher must acknowledge and agree not to publish the PHI in a form that could reasonably enable a person to ascertain the identity of the individual;
- The researcher must acknowledge and agree not to make contact or attempt to make contact with the individual to whom the PHI relates, directly or indirectly, unless the consent of the individual to being contacted is first obtained in accordance with subsection 44(6) of *PHIPA.*

Compliance with Statutory Requirements for the Disclosure for Research Purposes

This privacy policy indicates that the Research Agreement must require the researcher and HHS/CritiCall to acknowledge and agree that the researcher has submitted an application in writing, a written research plan that meets the requirements of the *Act* and its regulation, and a copy of the decision of the research ethics board approving the written research plan. The Research Agreement includes this requirement.

This privacy policy requires that the researcher acknowledge and agree that the researcher will comply with the Research Agreement, with the written research plan approved by the research ethics board and with the conditions, if any, specified by the research ethics board in respect of the written research plan. The Research Agreement includes this requirement.

Secure Transfer of PHI

This policy requires the Research Agreement to identify the manner in which records of PHI, which will be disclosed pursuant to the Research Agreement, are securely transferred. The policy also requires the Research Agreement to set out the secure manner in which records of PHI will be transferred, including under what conditions and to whom the records will be transferred, and the procedures that will be followed in ensuring that the records of PHI are transferred in a secure manner. In identifying the secure manner in which the records of PHI will be transferred, the Research Agreement must have regard to the *S-7 Policy and Procedures for Secure Transfer of Records of Personal Health Information* implemented by HHS/CritiCall. The Research Agreement includes this requirement.

This privacy policy and the Research Agreement requires that HHS/CritiCall and the researcher acknowledge and agree that:

1. Where it is necessary to transfer records of PHI to or from HHS/CritiCall the Recipient must comply with *S7: Policy and Procedures for the Secure Transfer of Personal Health Information* and must transfer the records in a secure manner in keeping with HHS/CritiCall policies and procedures as outlined in Appendix "A" of the Research Agreement - Relevant Policies and Procedures which may be amended from time to time; and
2. An encrypted and password-protected compact disk or media shall be used for the secure transfer of any PHI from HHS/CritiCall to the Recipient or from the Recipient to HHS/CritiCall.

Secure Retention of PHI

This privacy policy requires that the retention period for the records of PHI subject to the Research Agreement must be identified in the Research Agreement, including the length of time that the records of PHI will be retained in identifiable form. This policy requires the retention period identified in the Research Agreement to match the retention period set out in the written research plan, approved by the research ethics board. The Research Agreement includes this requirement.

This policy indicates that the Research Agreement shall require the researcher to ensure that the records of PHI are retained in a secure manner and shall identify the precise manner in which the records of PHI in paper and electronic format will be securely retained. In identifying the secure manner in which the records of PHI will be retained, the Research Agreement has regard to the P5:

Policy and Procedures for Secure Retention of Records of Personal Health Information and must have regard to the written research plan approved by the research ethics board. The Research Agreement includes this requirement.

This policy requires the Research Agreement to indicate that the researcher must take steps that are reasonable in the circumstances to ensure that the PHI subject to the Research Agreement is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of PHI subject to the Research Agreement are protected against unauthorized copying, modification or disposal. The reasonable steps that are required to be taken by the researcher must be detailed in the Research Agreement and, at a minimum, must include those set out in the written research plan approved by the research ethics boards. The Research Agreement includes this requirement.

Secure Return or Disposal

This privacy policy requires the Research Agreement to include the definition for "secure disposal" that is consistent with *PHIPA* and its regulation and identifies the precise manner in which the records of PHI must be securely disposed of. The Research Agreement includes this requirement.

This privacy policy requires and the Research Agreement states that the researcher shall, unless otherwise expressly authorized by HHS/CritiCall, in writing, undertake and ensure the secure destruction of PHI in the researcher's custody or control within five (5) days after the first of the following occur:

- The termination of the Research Agreement for any reason;
- The provision of a written request from HHS/CritiCall to the researcher to undertake the secure destruction of the PHI; or
- The date expressly specified for secure destruction of the PHI in the Research Agreement.

This privacy policy and the Research Agreement require the researcher to provide the Executive Director, CritiCall with written confirmation in the form of a certificate of destruction of the secure destruction of the PHI within 30 days of destruction. The written confirmation shall:

- Identify the PHI that was destroyed;
- Specify the date, time, location, and method of secure destruction employed;
- Bear the name and signature of the person who performed the secure destruction and a witness; and
- Be provided to the CritiCall Executive Director, no later than 30 days after the secure destruction of the PHI.

This privacy policy requires and the Research Agreement indicates that when performing the secure destruction of PHI, the researcher will ensure the method of secure disposal employed is consistent with *PHIPA* and Regulation 329/04; with Orders issued by the IPC under *PHIPA* and its Regulation, including Order HO-001 and Order HO-006; with guidelines, fact sheets and best practices issued by the IPC pursuant to *PHIPA* and its Regulation, including Fact Sheet 10: Secure Destruction of Personal Information; and with the policies and procedures set out in Appendix "A" Relevant Policies and Procedures and specifically *S8: Policy and Procedures for Secure Disposal of Records of*

Personal Health Information which may be amended from time to time. Additional guidelines and requirements for secure disposal are set out in "Appendix B".

As per this privacy policy and the Research Agreement, in the event that the researcher is unable to ensure the secure destruction of PHI the researcher shall promptly provide the Executive Director, CritiCall with a written explanation of the factors preventing the secure destruction of the PHI. HHS/CritiCall may, in its sole discretion, direct the researcher to transfer the PHI to HHS/CritiCall in a secure manner using the methods that HHS/CritiCall in its sole discretion may direct.

This privacy policy and the Research Agreement state that if the records of PHI are required to be de-identified and retained by the researcher rather than being securely returned or disposed of, the manner and process for de- identification must be set out in the Research Agreement. In identifying the manner and process for de-identification, regard may be had to the *Policy and Procedures with Respect to De- Identification and Aggregation* implemented by HHS/CritiCall. The Research Agreement also requires the researcher to submit written confirmation that the records were de-identified and shall stipulate the timeframe following the retention period set out in the Research Agreement within which the written confirmation must be provided and the agent of the prescribed person or prescribed entity to whom the written confirmation must be provided.

Notification

This policy states and the Research Agreement indicates that if a breach occurs or there is a suspected breach, the researcher must provide the CritiCall Privacy Lead with all of the information within the researcher's knowledge about the breach or suspected breach in writing, immediately after the researcher becomes aware:

- That there has been any suspected breach of the researchers duties under *PHIPA*;
- Any breach or suspected breach of a term or condition of the Research Agreement which for greater clarity, includes all appendices to the Research Agreement; or
- There has been any breach or suspected breach of section 44(6) of *PHIPA*.

This privacy policy requires that the Research Agreement indicate that researchers comply with *P29: Policy and Procedures for Privacy Breach Management* or *S17: Policy and Procedures for Security Breach Management* and:

- Immediately notify HHS/CritiCall if the PHI subject to the Research Agreement is stolen, lost, or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons by contacting the CCIS Help Desk by telephoning: 1-866-740-3240 and reporting the actual or suspected breach;
- Take steps that are reasonable in the circumstances to contain the breach in addition to containing any theft, loss or unauthorized access;
- Cooperate with HHS/CritiCall in the investigation and report of any such incident which may include but not be limited to documenting the circumstances of the incident and providing such written report to HHS/CritiCall; and
- Take any action as required based on the outcome of the investigation.

Consequences of Breach and Monitoring Compliance

This privacy policy requires the Research Agreement to outline the consequences of a breach of the agreement. This policy states that the Research Agreement must require the Researcher to provide reasonable assurances of compliance with the Agreement. This Research Agreement permits HHS/CritiCall, to, in its sole discretion and upon notice of not less than seven (7) days, conduct an audit to ensure the Researcher's compliance with the Agreement. Further, this Research Agreement outlines that an audit may include, but is not limited to, provision of Agreements and inspection of premises or computer databases to confirm that security and privacy controls are in place. HHS/CritiCall shall provide a copy of the audit report to the Researcher as well as a copy of the remediation plan developed by HHS/CritiCall to address any deficiencies identified in the audit report. The remediation plan will list the action items and timing proposed to address any identified deficiencies.

This policy states that the Research Agreement must also require the researcher to ensure that all persons who will have access to the PHI, as identified in the written research plan approved by the research ethics board, are aware of and agree to comply with the terms and conditions of the Research Agreement prior to being given access to the PHI. The Research Agreement must set out the method by which this will be ensured by the researcher, such as requiring the persons identified in the written research plan to sign an acknowledgement prior to being granted access, indicating that they are aware of and agree to comply with the terms and conditions of the Research Agreement.

P15. LOG OF RESEARCH AGREEMENTS

HHS/CritiCall has implemented and maintains a log of executed Research Agreements. The log is maintained by the CritiCall Privacy Lead includes the following information:

- The name of the research study;
- The name of the principal investigator to whom the PHI was disclosed pursuant to the Research Agreement;
- The date(s) of receipt of the written application, the written research plan and the written decision of the research ethics board approving the research plan;
- The date that the approval to disclose the PHI for research purposes was granted by HHS/CritiCall;
- The date that the Research Agreement was executed;
- The date that the PHI was disclosed;
- The nature of the PHI disclosed;
- The retention period for the records of PHI as set out in the Research Agreement;
- Whether the records of PHI will be securely returned, securely disposed of or de-identified and retained by the researcher following the retention period set out in the Research Agreement; and
- The date that the records of PHI were securely returned, a certificate of destruction was received or written confirmation of de-identification was received or the date by which they must be returned, disposed of or de-identified.

P16. POLICY AND PROCEDURES FOR THE EXECUTION OF DATA SHARING AGREEMENTS

HHS/CritiCall has developed and implemented a policy and procedures for the execution of data sharing agreements. This policy and procedures provides direction for the identification of the circumstances requiring the execution of a Data Sharing Agreement and sets out the process and requirements for the execution of a Data Sharing Agreement.

This privacy policy requires a Data Sharing Agreement to be executed in the following circumstances:

- Prior to the collection of PHI for purposes other than research when a hospital with one or more Critical Care Units chooses to participate in the CCIS; or
- Prior to the disclosure of PHI for purposes other than research when an individual or organization has made a request for PHI which has been approved.

This privacy policy states that the Executive Director, CritiCall is responsible for ensuring that disclosure was approved in accordance with *P12*: *Policy and Procedures for Disclosure of Personal Health Information for Purposes Other Than Research;* collection of PHI was approved in accordance with the *P-4 Policy and Procedures for the Collection of Personal Health Information* for the execution of the Data Sharing Agreements; for maintaining the *P18: Log of Data Sharing Agreements;* and for retaining the signed original copy of the Data Sharing Agreements in a secure location.

This privacy policy identifies the CritiCall Privacy Lead as being responsible for ensuring that a Data Sharing Agreement is executed, as well as the process that must be followed and the requirements that must be satisfied in this regard. This policy outlines the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

The privacy policy indicates that the CritiCall Privacy Lead is responsible for maintaining a Log of Data Sharing Agreements. The Executive Director, CritiCall shall review the *P18: Log of Data Sharing Agreements* annually identifying any Agreements set to expire for the year ahead. The Executive Director is responsible for following the 'End of Term' procedures for any agreements set to expire.

Compliance

This privacy policy requires all HHS/CritiCall employees and agents to comply with this policy and procedure. The CritiCall Privacy Lead is responsible for the enforcement of this policy and procedure. This privacy policy and procedures addresses the consequence of a breach.

This privacy policy requires the HHS Legal Counsel and Chief Privacy Officer, or delegate and the CritiCall Privacy Lead to conduct an annual audit of this policy and procedure in accordance with the *P-28 Policy and Procedures in Respect of Privacy Audits*. 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 Legal Counsel and Chief Privacy Officer. The HHS Legal Counsel and Chief Privacy Officer or delegate may conduct additional random audits at any time. The audit criteria and reporting requirements are further outlined within the *P27: Policy and Procedures In Respect of Privacy Audits*.

This privacy policy states that if a breach or suspected breach of this policy is found to have occurred an investigation will be conducted by the CritiCall Privacy Lead. If a breach, a suspected breach or a privacy risk with regard to collection or 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 in accordance with the *P-29 Policy and Procedures for Privacy Breach Management*. 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 Procedures for Privacy Breach Management*.

P17. TEMPLATE DATA SHARING AGREEMENT

HHS/CritiCall has developed and implemented a policy and procedures for the execution of data sharing agreements and a template Data Sharing Agreement that addresses the criteria below.

General Provisions

The Template Data Sharing Agreement identifies HHS, as a *prescribed person* in respect of the CCIS as per section 13(1) of O. Reg. 329/04 enacted under *PHIPA*. This Template Data Sharing Agreement states that pursuant to section 39(1)(c) of *PHIPA* a prescribed person compiles or maintains a registry for the purposes of facilitating or improving the provision of health care and specifies the duties and responsibilities arising from this status.

This privacy policy indicates that HHS/CritiCall's requires that a Data Sharing Agreement is executed in the circumstances set out in the *P-16 Policy and Procedures for the Execution of Data Sharing Agreements* that address all components provided in the policy and procedures.

This Template Data Sharing Agreement requires that the precise nature of the PHI subject to the Data Sharing Agreement is specified and a definition of PHI is included which is consistent with *PHIPA* and its regulation. The Template Data Sharing Agreement requires that the Data Sharing Agreement identifies the person or organization that is collecting PHI and the person or organization that is disclosing PHI pursuant to the Data Sharing Agreement.

Purposes of Collection, Use and Disclosure

The Template Data Sharing Agreement requires that the Data Sharing Agreements identify the purpose for which the PHI subject to the Data Sharing Agreement is being collected and for which purpose the PHI will be used. The Template Data Sharing Agreement also states that PHI disclosed and collected pursuant to the Data Sharing Agreement is necessary for the purpose for which it is disclosed and collected and other information, de-identified and/or aggregate information will not serve the purpose. The Template Data Sharing Agreement contains an acknowledgement that no more PHI is being collected or used than is reasonably necessary to meet the purpose.

The collection, use and disclosure of PHI subject to the Data Sharing Agreement will comply with the provisions of *PHIPA* and its Regulation. The Template Data Sharing Agreement requires all persons who will have access to the PHI to sign a Confidentiality Agreement and comply with the terms of the Data Sharing Agreement.

The Template Data Sharing Agreement requires that the Data Sharing Agreements explicitly state whether or not the PHI collected pursuant to the Data Sharing Agreement will be linked to other information. If the PHI will be linked to other information, the Template Data Sharing Agreement states that the Data Sharing Agreement must identify the nature of the information to which the PHI will be linked, the source of the information to which the PHI will be linked, how the linkage will be conducted and why the linkage is required for the identified purposes.

The Template Data Sharing Agreement requires that the Data Sharing Agreements also identify the purposes, if any, for which the PHI subject to the Data Sharing Agreement may be disclosed and any limitations, conditions or restrictions imposed thereon.

The Template Data Sharing Agreement requires the collection, use and disclosure of PHI subject to the Data Sharing Agreement to comply with the *Act* and its regulation and must set out the specific statutory authority for each collection, use and disclosure contemplated in the Data Sharing Agreement.

Secure Transfer

This privacy policy requires the Data Sharing Agreement to state that the Parties will mutually determine the method, medium, frequency including under what conditions and to whom the records will be transferred, and the procedure that must be followed in ensuring that the records are transferred in a secure manner and timetable to be used with respect to the provision of information under the Data Sharing Agreement. The secure manner in which records of PHI are transferred must be agreed upon in the Data Sharing Agreement prior to the secure transfer of PHI. In identifying the secure manner in which the records of PHI will be transferred, regard may be had to the S-7 *Policy and Procedures for Secure Transfer of Records of Personal Health Information* implemented by HHS/CritiCall.

This template Data Sharing Agreement indicates that the requestor of PHI is required to take reasonable steps to protect PHI during use, storage and transmission from theft, loss, unauthorized use or disclosure, unauthorized copying, modification, or disposal, by means of industry best practices, including encryption, audit trails, intrusion and alteration alert systems.

Secure Retention

The template Data Sharing Agreement requires that the requestor of PHI retain the PHI subject to the Data Sharing Agreement for a specified time and only for as long as is necessary to fulfill the purposes for which the records of PHI were collected. In addition, this privacy policy requires the Data Sharing Agreement to outline whether the PHI will be retained via electronic or paper format and whether they will be in an identifiable form. The Data Sharing Agreement requires the PHI to be stored in a secure manner, in a physically secure location with restricted access. In identifying the secure manner in which the records of PHI will be retained, the Data Sharing Agreement has regard to the *S5- Policy and Procedures for Secure Retention of Records of PHI.*

The Data Sharing Agreement requires that the requestor take reasonable steps to ensure that the PHI subject to the Data Sharing Agreement is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of PHI are protected against unauthorized copying, modification or disposal by means of industry best practices, including encryption, audit trails, intrusion and alteration alert systems. The reasonable steps to be taken are detailed in the Data Sharing Agreement and include physical and administrative controls including locked premises, employee training requirements and the execution of confidentiality agreements for all agents prior to being granted access to PHI.

Secure Return or Disposal

The Data Sharing Agreement addresses whether the records of PHI subject to the Data Sharing Agreement will be returned in a secure manner or will be disposed of in a secure manner following the retention period set out in the Data Sharing Agreement or following the date of termination of the Data Sharing Agreement, as the case may be.

If the records of PHI are required to be returned in a secure manner, the Data Sharing Agreement must stipulate the time frame following the retention period or following the date of termination of the Data Sharing Agreement within which the records of PHI must be securely returned, the secure manner in which the records must be returned and the person to whom the records must be securely returned. In identifying the secure manner in which the records of PHI will be returned, regard may be had to the S-7 *Policy and Procedures for Secure Transfer of Records of Personal Health Information* implemented by HHS/CritiCall.

This privacy policy states that if the records of PHI are required to be disposed of in a secure manner, the Data Sharing Agreement must provide a definition of secure disposal that is consistent with the *Act* and its regulation and must identify the precise manner in which the records of PHI subject to the Data Sharing Agreement must be securely disposed of. The Data Sharing Agreement must also stipulate the time frame following the retention period or following the date of termination of the Data Sharing Agreement within which the records of PHI must be securely disposed of and within which a certificate of destruction must be provided.

In identifying the secure manner in which the records of PHI will be disposed of, it must be ensured that the method of secure disposal identified is consistent with the *Act* and its regulation; with orders and decisions issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the IPC pursuant to the *Act* and its regulation, including *Fact Sheet 10: Secure Destruction of Personal Information*. In addition, regard may be had to the *S-8 Policy and Procedures for Secure Disposal of Records of Personal Health Information* implemented by HHS/CritiCall.

Further, the Data Sharing Agreement identifies the Executive Director, CritiCall as being the person to whom the certificate of destruction must be provided, the time frame following secure disposal within which the certificate of destruction must be provided and the required content of the certificate of destruction. At a minimum, the certificate of destruction must identify the records of PHI securely disposed of; to stipulate the date, time, location and method of secure disposal employed; and to bear the name and signature of the person who performed the secure disposal.

Notification

This privacy policy requires the Data Sharing Agreement to include a clause which requires notification be provided at the first reasonable opportunity if the Data Sharing Agreement has been breached or is suspected to have been breached or if the PHI subject to the Data Sharing Agreement is stolen, lost or accessed by unauthorized persons or is believed to have been stolen, lost or accessed by unauthorized persons. It also identifies whether the notification must be verbal and/or in writing and to whom the notification must be provided. The Data Sharing Agreement also requires that reasonable steps be taken to contain the breach of the Data Sharing Agreement and to contain the theft, loss or access by unauthorized persons.

Consequences of Breach and Monitoring Compliance

This privacy policy requires the Data Sharing Agreement to outline the consequences of a breach of the agreement and must indicate whether compliance with the Data Sharing Agreement will be audited and, if so, the manner in which compliance will be audited and the notice, if any, that will be provided of the audit.

This Data Sharing Agreement requires that all persons who will have access to the PHI are aware of and agree to comply with the terms and conditions of the Data Sharing Agreement prior to being given access to the PHI. As per this privacy policy this Data Sharing Agreement must set out the method by which this will be ensured. This may include requiring the persons that will have access to the PHI to sign an acknowledgement, prior to being granted access, indicating that they are aware of and agree to comply with the terms and conditions of the Data Sharing Agreement.

P18. LOG OF DATA SHARING AGREEMENTS

HHS/CritiCall has implemented and maintains a log of executed Data Sharing Agreements. The log is maintained by the Executive Director, CritiCall, or delegate and includes:

- The name of the person or organization from whom the PHI was collected or to whom the PHI was disclosed;
- The date that the collection or disclosure of PHI was approved;
- The date that the Data Sharing Agreement was executed;
- The date the PHI was collected or disclosed;
- The nature of the PHI subject to this Data Sharing Agreement;
- The retention period for the records of PHI set out in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement;
- Whether the records of PHI will be securely returned or securely disposed of following the retention period set out in the Data Sharing Agreement, or the date of termination of the Data Sharing Agreements; and
- The date the records of PHI were securely returned or a certificate of destruction was provided or the date by which they must be returned or disposed of.

P19. POLICY AND PROCEDURES FOR EXECUTING AGREEMENTS WITH THIRD PARTY SERVICE PROVIDERS IN RESPECT OF PERSONAL HEALTH INFORMATION

HHS/CritiCall has developed and implemented a policy and procedures for executing agreements with third party service providers in respect of PHI. This privacy policy requires HHS/CritiCall to enter into written agreements with third party service providers prior to permitting third party service providers to access and use the PHI of HHS/CritiCall. This privacy policy and procedures includes the process that must be followed and the requirements that must be satisfied prior to the execution of written agreements. This privacy policy requires written agreements with third party service providers to access and use the PHI in CCIS to include the standard *P20: Template Agreement for All Third Party Service Providers* language.

This privacy policy and procedures requires the Executive Director, CritiCall to ensure that HHS/CritiCall will not provide PHI to a third party service provider if other information, namely de-identified and/or aggregate information, will serve the purpose and will ensure that when PHI is provided, HHS/CritiCall does not provide more PHI than is reasonably necessary to meet the purpose. The Executive Director, CritiCall is responsible for the execution of the Third Party Service Provider Agreements, for maintaining the *P21: Log of Agreements with Third Party Service Providers* and for retaining the signed original copy of the Third Party Service Provider Agreements in a secure location.

This privacy policy and procedures identifies the CritiCall Privacy Lead as being responsible for ensuring that records of PHI provided to a third party service provider are either securely returned to HHS/CritiCall or are securely disposed of, as the case may be, following the termination of the agreement. This privacy policy further addresses the process to be followed where records of PHI are not securely returned or a certificate of destruction is not received following the termination of the agreement, including the agent(s) responsible for implementing this process and the time frame following termination within which this process must be implemented.

This privacy policy and procedures requires that a log be maintained of all agreements executed with third party service providers and identifies the agent(s) responsible for maintaining such a log. In addition, this privacy policy and procedures addresses where documentation related to the execution of agreements with third party service providers will be retained and the agent(s) responsible for retaining this documentation.

This privacy policy and procedures requires HHS/CritiCall agents to comply with this policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. This policy and procedures stipulates that compliance will be audited in accordance with the *P-27 Policy and Procedures In Respect of Privacy Audits*, indicates that an annual audit will be conducted and identifies the CritiCall Privacy Lead as being responsible for conducting the audit and for ensuring compliance with this policy and its procedures.

This policy and procedures also requires agents to notify the CCIS HelpDesk at the first reasonable opportunity, in accordance with the *P-29 Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

P20. TEMPLATE AGREEMENT FOR ALL THIRD PARTY SERVICE PROVIDERS

HHS/CritiCall has created a template for agreements with third party service providers that are permitted to access and use PHI including those that are contracted to retain, transfer or dispose of records of PHI and those that are contracted to provide services for the purpose of enabling HHS/CritiCall to use electronic means to collect, use, modify, disclose, retain or dispose of PHI.

General Provisions

This privacy policy and procedures describes the status of HHS/CritiCall as a prescribed person under *PHIPA* and outlines the duties and responsibilities arising from this status.

This privacy policy and procedures provides that all third party service providers that are permitted to access and use PHI in the course of providing services to HHS/CritiCall shall be considered agents of HHS/CritiCall, with the possible exception of electronic service providers. Agreements with electronic service providers shall explicitly state whether or not the third party service provider is an agent of HHS/CritiCall in providing services pursuant to the agreement. The third party agrees in all its dealings with PHI and CCIS data in general, to comply with the provisions of *PHIPA* and its Regulation, and with HHS/CritiCall's privacy and security policies and procedures.

This privacy policy and procedures requires that the agreement provide a definition of PHI and that the definition provided be consistent with the *Act* and its regulation. Where appropriate, the agreement must also specify the precise nature of the PHI that the third party service provider will be permitted to access and use in the course of providing services pursuant to the agreement.

The agreement must also require that the services provided by the third party service provider pursuant to the agreement be performed in a professional manner, in accordance with industry standards and practices, and by properly trained agents of the third party service provider.

Obligations with Respect to Access and Use

This privacy policy and procedures requires the agreement to identify the purposes for which the third party service provider is permitted to access and use the PHI of HHS/CritiCall and any limitations, conditions or restrictions imposed thereon. The template agreement also includes the following information:

- The authority under *PHIPA* and its Regulation for each permitted access to and use of PHI;
- A stipulation that the third party may not access or use PHI for any other purpose than those set out in the agreement;
- If the agreement is with an electronic service provider that is not an agent of HHS/CritiCall, the agreement must explicitly prohibit the electronic service provider from using PHI except as necessary in the course of providing services pursuant to the agreement. As such the third party acknowledges that it is not an agent of HHS/CritiCall and will adhere to the requirement prescribed in section 6 of the Regulation enacted under *PHIPA*;
- A statement prohibiting the third party from accessing or using PHI if other information will suffice; and

- A statement prohibiting the third party from using more PHI than if other information will serve the purpose and from using more PHI than is reasonably necessary to meet the purpose.

Obligations with Respect to Disclosure

This privacy policy and procedures requires the agreement to identify the purposes, if any, for which the third party service provider is permitted to disclose the PHI of HHS/CritiCall and any limitations, conditions or restrictions imposed thereon.

In identifying the purposes for which the third party service provider is permitted to disclose PHI, HHS/CritiCall must ensure that, each disclosure identified in the agreement is consistent with the disclosures of PHI permitted by the *Act* and its regulation. In this regard, the agreement prohibits the third party service provider from disclosing PHI except as permitted in the agreement or as required by law, from disclosing PHI if other information will serve the purpose and from disclosing more PHI than is reasonably necessary to meet the purpose.

This privacy policy and procedures indicates that in the case of an electronic service provider that is not an agent of HHS/CritiCall, the agreement must prohibit the electronic service provider from disclosing PHI to which it has access in the course of providing services except as required by law.

Secure Transfer

This privacy policy and procedures states that to transfer records of PHI to or from HHS/CritiCall, the agreement must require the third party service provider to securely transfer the records of PHI and must set out the responsibilities of the third party service provider in this regard. The template includes the following information:

- A stipulation that PHI must be transferred by the third party in a secure manner where it is necessary to transfer PHI;
- A stipulation that no records of PHI that have been accessed and used by the third party shall be retained if other records will serve the purpose;
- A description of the manner in which PHI is permitted to be transferred by the third party and the procedures for this manner of transfer with reference to *S7: Policy and Procedures for the Secure Transfer of Personal Health Information* implemented by HHS/CritiCall;
- A list of conditions under which PHI is permitted to be transferred by the third party;
- Indications of to whom PHI is permitted to be transferred by the third party;
- A stipulation that third parties whose primary service is the storage or disposal of PHI must provide HHS/CritiCall with documentation stating the date, time and mode of transfer of PHI and confirming receipt of PHI by third party; and
- A stipulation that the third party must maintain an inventory of documentation relating to the transfer of PHI.

Secure Retention

The agreement shall require the third party service provider to retain the records of PHI, where applicable, in a secure manner and shall identify the precise methods by which records of PHI in

paper and electronic format will be securely retained by the third party service provider, including records of PHI retained on various media.

The agreement outlines the responsibilities of the third party service provider in securely retaining the records of PHI. In identifying the secure manner in which the records of PHI will be retained, and the methods by which the records of PHI will be securely retained, the agreement shall have regard to the *S-5 Policy and Procedures for Secure Retention of Records of Personal Health Information* implemented by HHS/CritiCall.

The template includes the following information:

- A stipulation that PHI must be retained by the third party in a secure manner where it is necessary to retain PHI;
- The third party must comply with *S5: Policy and Procedures for the Secure Retention of Personal Health Information* and retain records of PHI in a secure manner that includes encryption, audit trails and physical security systems; and
- Where the retention of records of PHI is the primary service provided to HHS/CritiCall by the third party service provider, the agreement must also obligate the third party service provider to maintain a detailed inventory of the records of PHI being retained on behalf of HHS/CritiCall as well as a method to track the records being retained which shall be made available to HHS/CritiCall on request.

Secure Return or Disposal Following Termination of the Agreement

This agreement addresses, where applicable, whether records of PHI will be securely returned to HHS/CritiCall or will be disposed of in a secure manner following the termination of the agreement. The agreement template includes the following information:

- An indication of whether records of PHI will be returned to HHS/CritiCall or disposed of in a secure manner by the third party following the termination of the agreement;
- If the PHI is required to be returned to HHS/CritiCall in a secure manner, the agreement must set out the time frame,30 days, and the manner in which the PHI must be returned and the HHS/CritiCall agent to whom the PHI must be returned to. In identifying the secure manner in which the records of PHI will be returned, the agreement shall have regard to the *S-7 Policy and Procedures for Secure Transfer of Records of Personal Health Information*;
- If the PHI is to be disposed of by the third party in a secure manner, the agreement must provide a definition of "secure disposal" that is consistent with the Act and its regulation and must identify the precise manner in which records of PHI are to be securely disposed of;
- A stipulation that in identifying the secure manner in which the records of PHI will be disposed of, it must be ensured that the method of secure disposal identified is consistent with the Act and its regulation; with orders issued by the IPC under the Act and its regulation, including Order HO-001 and Order HO-006; with guidelines, fact sheets and best practices issued by the IPC pursuant to the Act and its regulation, including *Fact Sheet 10: Secure Destruction of Personal Health Information*; and with the *S-8 Policy and Procedures for Secure Disposal of Records of Personal Health Information* implemented by HHS/CritiCall.
- A statement setting out the time frame following termination of the agreement within which the records of PHI must be securely disposed of and within which a certificate of destruction must be provided to HHS/CritiCall by the third party;

- The agreement requires a certificate of destruction (at a minimum, the certificate must identify the records of PHI securely disposed of; the date, time and method of secure disposal employed; the name and signature of the person who performed the secure disposal), and the particular HHS/CritiCall agent to whom a certificate must be provided.

Secure Disposal as a Contracted Service

This privacy policy requires that where the disposal of records of PHI is the primary service provided to HHS/CritiCall by the third party service provider, in addition to the requirements set out above in relation to secure disposal, the agreement sets out the responsibilities of the third party service provider in securely disposing of the records of PHI, including:

- The time frame within which the records are required to be securely disposed of;
- The precise method by which records in paper and/or electronic format must be securely disposed of, including records retained on various media;
- The conditions pursuant to which the records will be securely disposed of; and The person(s) responsible for ensuring the secure disposal of the records.

The agreement also enables HHS/CritiCall, at its discretion, to witness the secure disposal of the records of PHI subject to such reasonable terms or conditions as may be required in the circumstances.

Implementation of Safeguards

The agreement requires the third party service provider to take steps that are reasonable in the circumstances to ensure PHI accessed and used in the course of providing services set out in the agreement is protected against theft, loss, unauthorized use or disclosure, and unauthorized copying modification and disposal. The reasonable steps that are required to be implemented by the third party are also detailed in the agreement.

Training of Agents of the Third Party Service Provider

There is a stipulation in the agreement that the third party service provider must provide training to its agents on the importance of protecting the privacy of individuals whose PHI is accessed and used in the course of providing services pursuant to the agreement and on the consequences that may arise in the event of a breach of these obligations. In addition, a stipulation is included in the agreement that requires the third party service provider to ensure its agents who will have access to PHI are aware of and agree to comply with the terms and conditions of the agreement prior to being given access.

The method in which the third party service provider ensures its agents are aware of and agree to comply with the terms and conditions of the agreement prior to being given access to the PHI, is also included in the agreement.

Subcontracting of the Services

This privacy policy and procedures stipulates that in the event the agreement permits the third party service provider to subcontract the services provided under the agreement, the third party service provider must be required to acknowledge and agree that it will provide HHS/CritiCall with advance notice of its intention to do so, that the third party service provider will enter into a written agreement with the subcontractor on terms consistent with its obligations to HHS/CritiCall and that a copy of the written agreement will be provided to HHS/CritiCall.

Notification

The agreement requires that the third party notify the CritiCall Privacy Lead in writing at the first reasonable opportunity if there has been a breach or suspected breach of the agreement or if the PHI to which it has permission to access and/or use has been stolen, lost or accessed by unauthorized persons and shall comply with *P29: Policy and Procedures for Privacy Breach Management* or *S17: Policy and Procedures for Security Breach Management.* In addition, the third party service provider agrees to cooperate with HHS/CritiCall in the investigation and report of any such incidents including but not limited to documenting the circumstances of the incident and providing such written report to HHS/CritiCall. In such an event, the third party service provider must take all reasonable steps to contain and mitigate the breach of contract or of the PHI.

Consequences of Breach and Monitoring Compliance

This privacy policy and procedures requires that the third party service provider acknowledge and agree that HHS/CritiCall reserves the right to conduct an on-site audit of the services provided by the third parting including compliance with the agreement and relevant policies and procedures provided that HHS/CritiCall gives five (5) days' notice of the intention to conduct an audit; and that HHS/CritiCall may take action in the event that it determines that there has been a breach of the agreement. This action includes up to and including termination of the agreement.

P21. LOG OF AGREEMENTS WITH THIRD PARTY SERVICE PROVIDERS

HHS/CritiCall has implemented and maintains a log of agreements with third party service providers. The CritiCall Privacy Lead is responsible for maintaining a log of executed agreements with third party service providers. This log is maintained in an access-restricted location on the CritiCall shared operations drive and includes the following information:

- The name of the third party service provider;
- The nature of the services provided by the third party service provider that require access to and use of PHI;
- The date that the agreement with the third party service provider was executed;
- The date that the records of PHI or access to the records of PHI, if any, was provided;
- The nature of the PHI provided or to which access was provided;
- The date of termination of the agreement with the third party service provider;
- Whether the records of PHI, if any, will be securely returned or will be securely disposed of following the date of termination of the agreement; and

- The date records of PHI were securely returned or a certificate of destruction was provided or the date that access to the PHI was terminated or the date by which the records of PHI must be returned or disposed of or access terminated.

P22. POLICY AND PROCEDURES FOR THE LINKAGE OF RECORDS OF PERSONAL HEALTH INFORMATION

HHS/CritiCall has developed and implemented a privacy policy and procedures for the linkage of records of PHI. This policy and procedures states that HHS/CritiCall permits the linkage of records of PHI from the CCIS only in accordance with the purposes and circumstances detailed in this policy. Any linkage of data that is not in accordance with the terms and conditions of this policy and related procedures is expressly prohibited.

This privacy policy and procedures states that the linkage of records of PHI is permitted for the purpose of supporting research and projects that have been reviewed and approved by the CCIS Data Stewardship Committee and deemed to be in alignment with the purpose of the CCIS as stated in *P7: Statement of Purpose for Data Holdings Containing Personal Health Information.*

This privacy policy and procedures states that in identifying the purposes for which and the circumstances in which the linkage of records of PHI is permitted, regard must be had to the sources of the records of PHI that are requested to be linked and the identity of the person or organization that will ultimately make use of the linked records of PHI, including:

- The linkage of records of PHI solely in the custody of HHS/CritiCall for the exclusive use of the linked records of PHI by HHS/CritiCall;

- The linkage of records of PHI in the custody of HHS/CritiCall with records of PHI to be collected from another person or organization for the exclusive use of the linked records of PHI by HHS/CritiCall;

- The linkage of records of PHI solely in the custody of the prescribed person or prescribed entity for purposes of disclosure of the linked records of PHI to another person or organization; and

- The linkage of records of PHI in the custody of HHS/CritiCall with records of PHI to be collected from another person or organization for purposes of disclosure of the linked records of PHI to that other person or organization.

Review and Approval Process

This privacy policy and procedures identifies the CritiCall Privacy Lead and the CCIS Data Stewardship Committee as being responsible for receiving, reviewing and determining whether to approve or deny the request to link records of PHI and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or

executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

This privacy policy and procedures addresses the requirements that must be satisfied and the criteria that must be considered by the CritiCall Privacy Lead, who is responsible for determining whether to approve or deny the request to link records of PHI.

This privacy policy and procedures also sets out the manner in which the decision approving or denying the request to link records of PHI and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.

Conditions or Restrictions on the Approval

This privacy policy and procedures states that where the linked records of PHI will be disclosed by HHS/CritiCall to another person or organization, the policy and procedures requires that the disclosure be approved pursuant to the *P-13 Policy and Procedures for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements* or the *P-12 Policy and Procedures for Disclosure of Personal Health Information For Purposes Other Than Research*, as may be applicable.

Where the linked records of PHI will be used by HHS/CritiCall, the policy and procedures requires that the use be approved pursuant to the *P-10 Policy and Procedures for the Use of Personal Health Information for Research* or the *P-8 Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information*, as may be applicable. The policy and procedures further requires that the linked records of PHI be de-identified and/or aggregated as soon as practicable pursuant to the *P-24 Policy and Procedures with Respect to De-Identification and Aggregation* and that, to the extent possible, only de-identified and/or aggregate information be used by agents of HHS/CritiCall.

Process for the Linkage of Records of Personal Health Information

This privacy policy and procedures states researchers who receive approval to receive and link records of PHI from the CCIS are responsible for ensuring that the data linkage is performed in a manner and by an individual with the required knowledge and skill that meets the approval of the CCIS Data Stewardship Committee. This privacy policy and procedures outlines the manner in which the linkage of records of PHI must be conducted.

The requestor must provide the following information for review and approval by the CCIS Data Stewardship Committee:

- A description of the process for the linkage of data of PHI from the CCIS;
- The credentials of the individual(s) who will be performing the linkage;
- Any agent of HHS/CritiCall who performs data linkage must be appointed by the CritiCall Executive Director to perform this function and have the required knowledge and skills; and
- Prior to release of any kind, all linked records of PHI from the CCIS must be de-identified or aggregated in accordance with *P24: Policy and Procedures with Respect to De-Identification and Aggregation.*

Retention

This privacy policy and procedures requires any retention of PHI data from the CCIS to comply with *S5: Policy and Procedures for Secure Retention of Records of PHI* until they are de-identified and/or aggregated pursuant to the *Policy and Procedures with Respect to De-Identification and Aggregation.*

Secure Disposal

This privacy policy and procedures addresses the secure disposal of records of PHI from the CCIS linked by an agent of HHS/CritiCall and, in particular, requires that the records of PHI be securely disposed of in compliance with the *S-8 Policy and Procedures for Secure Disposal of Records of Personal Health Information.*

Compliance, Audit and Enforcement

This policy and procedures states that all HHS/CritiCall agents must comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of a breach.

This policy and procedures stipulates that the HHS Chief Privacy Officer, or delegate and the CritiCall Privacy Lead will conduct an annual audit of this policy and procedure in accordance with *P27: CCIS Policy and Procedures In Respect of Privacy Audits*. 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 Chief Privacy Officer. The HHS Chief Privacy Officer or delegate may conduct additional random audits at any time.

This privacy policy and procedures requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the *P-29 Policy and Procedures for Privacy Breach Management*, if an agent breaches or suspects there may have been a breach of this policy or its procedures.

Tracking Approved Linkages of Records of Personal Health Information

This privacy policy and procedures requires that a log be maintained of the linkages of records of PHI approved by the CCIS Data Stewardship Committee, which is the responsibility of the CritiCall Privacy Lead to maintain. This policy and procedures also addresses where documentation related to the receipt, review, approval or denial of requests to link records of PHI will be retained and the agent(s) responsible for retaining this documentation.

P23. LOG OF APPROVED LINKAGES OF RECORDS OF PERSONAL HEALTH INFORMATION

HHS/CritiCall has implemented and maintains a log of approved linkages of records of PHI. The CritiCall Privacy Lead is responsible for maintaining and updating the log. The log includes the following information:

- Name of the agent, person or organization who requested the linkage;
- The date that the linkage of records of PHI was approved; and

- The nature of the records of PHI linked.

P24. POLICY AND PROCEDURES WITH RESPECT TO DE-IDENTIFICATION AND AGGREGATION

This privacy policy and procedures has been developed and implemented by HHS/CritiCall with respect to de-identification and aggregation. This policy prohibits HHS/CritiCall from using or disclosing PHI if de-identified and/or aggregate information, will serve the identified purpose.

This privacy policy and procedures requires that cell-sizes of less than five and the exceptions thereto must be articulated. In articulating the policy with respect to cell-sizes of less than five, regard is had to the restrictions related to cell-sizes of less than five contained in Data Sharing Agreements, Research Agreements and written research plans pursuant to which the PHI was collected by HHS/CritiCall.

This privacy policy defines *de-identified information* as identifiable information that has been modified, removed or substituted in such a manner so that the identity of an individual cannot be determined by using a method that is reasonably foreseeable in the circumstances to re-identify the data; and *aggregate data* is defined as data that has been grouped together and which does not contain identifying information. The definitions adopted and the policy of HHS/CritiCall with respect to cell-sizes of less than five shall have regard to, and must be consistent with, the meaning of "identifying information" in subsection 4(2) of the *Act*.

This policy states that HHS/CritiCall shall not provide CCIS data of a cell-size less than five (5) unless there has been a formal external assessment of the risk of re-identification and the risk of re-identification is below the acceptable threshold as approved by the CCIS Data Stewardship Committee. In conducting its review and approval of the disclosure of such data, the CCIS Stewardship Committee must consider the terms and conditions specified in any relevant agreements and research plans to ensure adequate protection of this data.

Any de-identified and/or aggregated information, including information of cell sizes less than five, must be reviewed by the CritiCall Executive Director or delegate prior to use or disclosure in order to ensure that the information does not identify an individual and 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.

This privacy policy and procedures requires the following information, at minimum, to be removed, encrypted and/or truncated in order to constitute de-identified information:

- Full Name;
- Address (including postal code);
- Health Card Number;
- Medical Record Number;
- Date of Birth; and
- Gender.

The information must be grouped, collapsed or averaged in the following manner to constitute aggregate information:

- Date of birth to month and year only or to age or age group; and
- Admission date and date of discharge to month and year only.

As per the terms and conditions of agreements which must be signed prior to disclosure of de-identified or aggregate data, agents and those in receipt of de-identified or aggregate data are prohibited from using de-identified and/or aggregate information, including information in cell-sizes of less than five, to identify an individual. Further, this policy and procedures identifies the mechanisms implemented to ensure that the persons or organizations to whom de-identified and/or aggregate information is disclosed will not use the de-identified and/or aggregate information, either alone or with other information, to identify and individual.

The requesting party must complete the appropriate CCIS Data Request Form (either For Research or Not for Research) found on the CritiCall Ontario website. The form must be completed in full and shall provide sufficient detail to allow the CCIS Data Stewardship Committee to determine if the request should be approved or denied. The following details must be provided by the requestor:

- A description of the request including but not limited to the required data elements and the time frame for the data;
- The rationale for the request;
- The format for receipt of the data (hard copy or electronic);
- How the requestor intends to receive the data;
- A description of how the data will be used;
- Confirmation that the requestor is willing to sign an agreement that will set out the terms and conditions of the receipt of the data including that the requestor will not undertake an attempt to re-identify the data and will prohibit agents from doing the same; and
- If the request is for a cell size less than 5, confirmation that the requestor will undertake an external assessment for risk of re-identification of the data.

On receipt of the request, the CritiCall Privacy Lead shall review the request with the CritiCall Executive Director. The Executive Director shall schedule a meeting of the CCIS Data Stewardship Committee or add the request to an agenda of a previously scheduled CCIS Data Stewardship Committee for review.

The CCIS Data Stewardship Committee shall review all requests against the established criteria as follows:

- The rationale for access to the de-identified data is sound;
- The individual or organization requesting the data has committed to signing an agreement which will require the individual and any agent to refrain from undertaking an attempt to re-identify the data.
- The data elements requested are included in the CCIS data set
- The list of data elements requested does not include:
    - Full Name;
    - Address (including postal code);
    - Health Card Number;

- Medical Record Number;
- Date of Birth; and
- Gender.

- If the cell size is anticipated to be less than five (5), the requestor has confirmed the requirement for undertaking an external assessment of the risk of re-identification.

The request will be approved only if all criteria are answered 'yes'. If the request is denied, the CCIS Data Stewardship Committee shall confirm the rationale for the denial. If the request is for a cell size less than five (5), the CCIS Data Stewardship Committee shall advise that an external review must be undertaken.

The CritiCall Privacy Lead shall communicate the decision of the CCIS Data Stewardship Committee to the requestor including the rationale for denial, if any, and if cell size is less than 5, communicate the requirement to proceed to an external review of the risk of re-identification.

On approval of the request, the CritiCall Executive Director shall notify the CCIS Product Manager. The CCIS Product Manager shall make arrangements to have the de-identified data prepared, consulting with a third party service provider as required. The Privacy Lead shall execute the required agreement prior to the release of data.

This policy and procedures stipulates that HHS/CritiCall requires agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of a breach. The policy and procedures also stipulates that compliance will be audited on an annual basis in accordance with the *P-27 Policy and Procedures In Respect of Privacy Audits*, and identifies the CritiCall Privacy Lead as being responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

The policy and procedures requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the *P-29 Policy and Procedures for Privacy Breach Management*, if an agent breaches or suspects there may have been a breach of this policy or its procedures.

P25. PRIVACY IMPACT ASSESSMENT POLICY AND PROCEDURES

This privacy policy and procedures identifies the circumstances in which privacy impact assessments (PIA) are required to be conducted for the CCIS. In identifying the circumstances in which PIAs are required to be conducted, HHS/CritiCall must conduct PIAs on existing and proposed data holdings involving PHI and whenever a new or a change to an existing information system, technology or program involving PHI is contemplated.

This privacy policy and procedures stipulates the limited and specific circumstances in which PIAs are not required to be conducted on existing and proposed data holdings involving PHI and whenever a new or a change to an existing information system, technology or program involving PHI is contemplated, along with a rationale for why PIAs are not required. The policy and procedures also identifies the agent(s) responsible for making this determination and requires the determination and the reasons for the determination to be documented.

This privacy policy and procedures addresses the timing of PIAs. With respect to proposed data holdings involving PHI and new or changes to existing information systems, technologies or

programs involving PHI, this policy and procedures requires that PIAs be conducted at the conceptual design stage and that they be reviewed and amended, if necessary, during the detailed design and implementation stage. With respect to existing data holdings involving PHI, the policy and procedures requires that a timetable be developed by the CritiCall Privacy Lead to ensure PIAs are conducted.

This privacy policy and procedures stipulates that once PIAs have been completed, they must be reviewed on an ongoing basis in order to ensure that they continue to be accurate and continue to be consistent with the information practices of HHS/CritiCall. This privacy policy and procedures identifies the circumstances in which and the frequency with which PIAs are required to be reviewed.

This privacy policy and procedures identifies the CritiCall Privacy Lead as being responsible for, and the process that must be followed in identifying when PIAs are required; in identifying when PIAs are required to be reviewed in accordance with the policy and procedures; in ensuring that PIAs are conducted and completed; and in ensuring that PIAs are reviewed and amended, if necessary. The role of agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program are also identified in respect of PIAs.

This policy and procedures also stipulates the required content of PIAs. At a minimum, the PIA must be required to describe:

- The data holding, information system, technology or program at issue;
- The nature and type of PHI collected, used or disclosed or that is proposed to be collected, used or disclosed;
- The sources of the PHI;
- The purposes for which the PHI is collected, used or disclosed or is proposed to be collected, used or disclosed;
- The reason that the PHI is required for the purposes identified;
- The flows of the PHI;
- The statutory authority for each collection, use and disclosure of PHI identified;
- The limitations imposed on the collection, use and disclosure of the PHI;
- Whether or not the PHI is or will be linked to other information;
- The retention period for the records of PHI;
- The secure manner in which the records of PHI are or will be retained, transferred and disposed of;
- The functionality for logging access, use, modification and disclosure of the PHI and the functionality to audit logs for unauthorized use or disclosure;
- The risks to the privacy of individuals whose PHI is or will be part of the data holding, information system, technology or program and an assessment of the risks;
- Recommendations to address and eliminate or reduce the privacy risks identified; and
- The administrative, technical and physical safeguards implemented or proposed to be implemented to protect the PHI.

The process for addressing the recommendations arising from PIAs, including the agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and

ensuring the implementation of the recommendations, is outlined in this privacy policy and procedures.

This privacy policy and procedures requires that a log be maintained of PIAs that have been completed; that have been undertaken but that have not been completed; and that have not been undertaken. This privacy policy and procedures also identifies the agent(s) responsible for maintaining such a log.

This privacy policy and procedures requires that all HHS/CritiCall agents must comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of a breach. The policy and procedures also stipulates that compliance will be audited in accordance with the *P-29 Policy and Procedures In Respect of Privacy Audits*, sets out the frequency with which the policy and procedures will be audited and identifies the CritiCall Privacy Lead as being responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

This privacy policy and procedures requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or suspects there may have been a breach of this policy or its procedures.

In developing this privacy policy and procedures, regard was given to the *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*, published by the IPC.

P26. LOG OF PRIVACY IMPACT ASSESSMENTS

HHS/CritiCall has implemented and maintains a log of all PIAs that have been completed for the CCIS as well as PIAs that have been undertaken but that have not been completed. The CritiCall Privacy Lead is responsible for maintaining and updating the log. The log includes the following information: a description of the data holding, information system, technology, or program involving PHI that is at issue; the date that the PIA was completed or is expected to be completed; the agents responsible for completing or ensuring the completion of the PIA; the recommendations arising from the PIA; the agents responsible for addressing each recommendation, the date that each recommendation was or is expected to be addressed; and the manner in which each recommendation was or is expected to be addressed.

HHS/CritiCall maintains a log of PIAs that describes the CCIS data holding information system, technologies or programs involving PHI and of new or changes to existing CCIS information systems, and technologies or programs involving PHI for which PIAs have not been undertaken. For each CCIS data holding, information system, technology or program, the log either sets out the reason that a PIA will not be undertaken and the agents responsible for making this determination or sets out the date that the PIA is expected to be completed and the agents responsible for completing or ensuring the completion of the PIA.

P27. POLICY AND PROCEDURES IN RESPECT OF PRIVACY AUDITS

This privacy policy and procedures sets out the types, nature and frequency of privacy audits that are required to be conducted as well as the process for conducting and reporting audits in respect of the CCIS. This privacy policy and procedures sets out the purposes of each type of privacy audit. This privacy policy and procedures requires HHS/CritiCall to conduct audits to assess compliance with the privacy policies, procedures and practices implemented by HHS/CritiCall and audits of the agent(s) permitted to access and use PHI pursuant to *P8: Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information*.

With respect to each privacy audit that is required to be conducted, this privacy policy and procedures sets out the following particulars: the nature and scope of the privacy audit; that the CritiCall Privacy Lead is responsible for conducting the privacy audit; the frequency with which and the circumstances in which each privacy audit is required to be conducted. In this regard, the policy and procedures requires a privacy audit schedule to be developed and identifies the agent(s) responsible for developing the privacy audit schedule. Further, for each type of privacy audit that is required to be conducted, this privacy policy and procedures sets out the process to be followed in conducting the audit, which includes the criteria that must be considered in selecting the subject matter of the audit.

This privacy policy and procedures must be considered in selecting the subject matter of the audit and whether or not notification will be provided of the audit, and if so, the nature and content of the notification and to whom the notification must be provided. This policy and procedures further discusses the documentation that must be completed, provided and/or executed in undertaking each privacy audit; that the CritiCall Privacy Lead is responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

This privacy policy and procedures sets out that the day-to-day management of the privacy program rests with the CritiCall Privacy Lead in consultation with the CritiCall Executive Director and the HHS Legal Counsel and Chief Privacy Officer. Day-to-day management of the security program rests with the CritiCall Security Lead in consultation with the CritiCall Executive Director and the HHS Chief Security Office (HHS CSO). Together the CritiCall Privacy and Security Leads are responsible for ensuring that the privacy and security audits are completed.

This privacy policy and procedures sets out the process that must be followed in addressing the recommendations arising from privacy audits, including that the CritiCall Privacy Lead is responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations.

This privacy policy and procedures also sets out the nature of the documentation that must be completed, provided and/or executed at the conclusion of the privacy audit, including the agent(s) responsible for completing, providing and/or executing the documentation, the agent(s) to whom the documentation must be provided and the required content of the documentation.

This privacy policy and procedures also sets out the manner and format in which the findings of privacy audits, including the recommendations arising from the privacy audits and the status of

addressing the recommendations, are communicated. This includes a discussion of the agent(s) responsible for communicating the findings of the privacy audit; the mechanism and format for communicating the findings of the privacy audit; the time frame within which the findings of the privacy audit must be communicated; and to whom the findings of the privacy audit will be communicated, including the HHS Chief Executive Officer or the CritiCall Executive Director.

This privacy policy and procedures further requires that a log be maintained of privacy audits and identifies the CritiCall Privacy Lead as being responsible for maintaining the log and for tracking that the recommendations arising from the privacy audits are addressed within the identified time frame. This policy and procedures further addresses where documentation related to privacy audits will be retained and the agent(s) responsible for retaining this documentation.

This privacy policy and procedures requires the agent responsible for conducting the privacy audit, to notify HHS/CritiCall at the first reasonable opportunity, of a privacy breach or suspected privacy breach in accordance with the *P-29 Policy and Procedures for Privacy Breach Management* and of an information security breach or suspected information security breach in accordance with the *S-17 Policy and Procedures for Information Security Breach Management.*

P28. LOG OF PRIVACY AUDITS

HHS/CritiCall has implemented and maintains a log of Privacy Audits. The CritiCall Privacy Lead is responsible for maintaining and updating the log. The log includes the following information:

- Nature and type of privacy audit conducted;
- The date the privacy audit was completed;
- The agent(s) responsible for completing the privacy audit;
- The recommendations arising from the privacy audit;
- The agent(s) responsible for addressing each recommendation;
- The date that each recommendation was or is expected to be addressed; and
- The manner in which each recommendation was or is expected to be addressed.

P29. POLICY AND PROCEDURES FOR PRIVACY BREACH MANAGEMENT

This privacy policy and procedures has been developed and implemented to address the identification, reporting, containment, notification, investigation and remediation of privacy breaches.

This policy and procedures provides a definition of the term “privacy breach” which includes the following:

- The collection, use and disclosure of PHI that is not in compliance with the *Act* or its regulation;
- A contravention of the privacy policies, procedures or practices implemented by HHS/CritiCall;
- The contravention of Data Sharing Agreements, Research Agreements, Confidentiality

Agreements and Agreements with Third Party Service Providers retained by HHS/CritiCall; and

- Circumstances where PHI is stolen, lost or subject to unauthorized use or disclosure or where records of PHI are subject to unauthorized copying, modification or disposal.

This privacy policy and procedures includes a mandatory requirement for agents to notify HHS/CritiCall of a privacy breach or suspected privacy breach.

In this regard, this policy and procedures identifies the CCIS HelpDesk as the agent to be notified of a privacy breach or suspected privacy breach and includes contact information for the CCIS HelpDesk. This policy and procedures stipulates that the agent notifying the CCIS HelpDesk of a privacy breach or suspected breach must do so at the first reasonable opportunity, which must be relayed either verbally and/or in writing or the nature of the information that must be provided upon notification. This policy and procedures also addresses the documentation that must be completed, provided and/or executed with respect to notification; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

Upon notification, this privacy policy and procedures requires a determination to be made of whether a privacy breach has in fact occurred and if so, what, if any, PHI has been breached. The CritiCall Privacy Lead is responsible for making this determination.

This privacy policy and procedures further addresses when senior management, including the HHS Chief Executive Officer or the CritiCall Executive Director, will be notified. This includes a discussion of the CritiCall Privacy Lead's responsibility for notifying senior management; the time frame within which notification must be provided; the manner in which this notification must be provided; and the nature of the information that must be provided to senior management upon notification.

This privacy policy and procedures also requires that containment be initiated immediately and identifies the CritiCall Executive Director, or delegate as being responsible for containment and the procedure that must be followed in this regard, including any documentation that must be completed, provided and/or executed by the agent(s) responsible for containing the breach and the required content of the documentation.

In undertaking containment, this privacy policy and procedures requires that reasonable steps are taken in the circumstances to protect PHI from further theft, loss or unauthorized use or disclosure and to protect records of PHI from further unauthorized copying, modification or disposal. This includes ensuring that no copies of the records of PHI have been made and ensuring that the records of PHI are either retrieved or disposed of in a secure manner. Where the records of PHI are securely disposed of, written confirmation should be obtained related to the date, time and method of secure disposal. These steps also include ensuring that additional privacy breaches cannot occur through the same means and determining whether the privacy breach would allow unauthorized access to any other information and, if necessary, taking further action to prevent additional privacy breaches.

This privacy policy and procedures states that the CritiCall Executive Director, or delegate is responsible and outlines the process to be followed in reviewing the containment measures implemented and determining whether the privacy breach has been effectively contained or whether

further containment measures are necessary. This privacy policy and procedures also addresses the documentation that must be completed, provided and/or executed by the agent(s) responsible for reviewing the containment measures; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

This privacy policy and procedures requires the health information custodian or other organization that disclosed the PHI to HHS/CritiCall to be notified at the first reasonable opportunity whenever PHI is or is believed to be stolen, lost or accessed by unauthorized persons and whenever required pursuant to the agreement with the health information custodian or other organization.

In particular, this privacy policy and procedures sets out the agent(s) responsible for notifying the health information custodian or other organization, the format of the notification and the nature of the information that must be provided upon notification. This privacy policy and procedures requires the health information custodian or other organization to be advised of the extent of the privacy breach, the nature of the PHI at issue, the measures implemented to contain the privacy breach and further actions that will be undertaken with respect to the privacy breach, including investigation and remediation. As a secondary collector of PHI, HHS/CritiCall does not directly notify the individual to whom the PHI relates of a privacy breach. This privacy policy and procedures requires notification to be provided by the health information custodian.

This privacy policy and procedures also sets out whether any other persons or organizations must be notified of the privacy breach and provides that the CritiCall Privacy Lead is responsible for notifying these other persons or organizations, the format of the notification, the nature of the information that must be provided upon notification and the time frame for notification.

This privacy policy and procedures identifies the CritiCall Privacy Lead as being responsible for investigating the privacy breach, the nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections) and the process that must be followed in investigating the privacy breach. This includes a discussion of the documentation that must be completed, provided and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation. The role of agent(s) that have been delegated day- to-day authority to manage the privacy program and the security program are also identified in this privacy policy and procedures.

The policy and procedures also identifies the CritiCall Privacy Lead as being responsible for assigning other agent(s) to address the recommendations; for establishing timelines to address the recommendations; for addressing the recommendations; and for monitoring and ensuring that the recommendations are implemented within the stated timelines. The policy and procedures also set out the nature of the documentation that must be completed, provided and/or executed at the conclusion of the investigation of the privacy breach, including the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

This privacy policy and procedures also addresses the manner and format in which the findings of the investigation of the privacy breach, including the recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This includes a discussion of the agent(s) responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within

which the findings of the investigation must be communicated; and to whom the findings of the investigation must be communicated, including the HHS Chief Executive Officer, and the CritiCall Executive Director..

In addition, this privacy policy and procedures addresses whether the process to be followed in identifying, reporting, containing, notifying, investigating and remediating a privacy breach is different where the breach is both a privacy breach or suspected privacy breach, as well as an information security breach or suspected information security breach.

This privacy policy and procedures requires that the CritiCall Privacy Lead must maintain a log of privacy breaches and the CritiCall Privacy Lead is responsible for tracking that the recommendations arising from the investigation of privacy breaches are addressed within the identified timelines. This privacy policy and procedures also sets out where documentation related to the identification, reporting, containment, notification, investigation and remediation of privacy breaches will be retained and the agent(s) responsible for retaining this documentation.

HHS/CritiCall requires all agents to comply with this privacy policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. This privacy policy and procedures also stipulates that compliance will be audited in accordance with the *P-28 Policy and Procedures In Respect of Privacy Audits*, sets out the frequency with which the policy and procedures will be audited and identifies the CritiCall Privacy Lead as responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

In developing this privacy policy and procedures, HHS/CritiCall had regard to the guidelines produced by the IPC entitled *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector*.

P30. LOG OF PRIVACY BREACHES

HHS/CritiCall has implemented and maintains a log of all Privacy Breaches. The CritiCall Privacy Lead is responsible for maintaining and updating the log. This privacy policy and procedures requires the log to include the following information:

- Date of privacy breach;
- Date the privacy breached was identified;
- Identifies whether the breach was an internal or external privacy breach;
- Nature of the PHI involved in the breach;
- Nature and extent of the breach;
- Date the privacy breach was contained;
- Nature of containment measures undertaken;
- Date of notification to HIC or Organization;
- Date investigation completed;
- Agent responsible for investigation;
- Recommendations;
- Agent responsible for addressing recommendations;
- Date each recommendation was or is expected to be addressed; and

- How recommendation was or is expected to be addressed.

P31. POLICY AND PROCEDURES FOR PRIVACY COMPLAINTS

This privacy policy and procedures has been developed and implemented to address the process to be followed in receiving, documenting, tracking, investigating, remediating and responding to privacy complaints. A definition of the term "privacy complaint" as 'a concern or complaint relating to the privacy policies, procedures and practices implemented by HHS/CritiCall related to the compliance of HHS/CritiCall for the CCIS with PHIPA and its regulation is included in this privacy policy and procedures.

This privacy policy and procedures outlines how information is communicated to the public relating to the manner in which, to whom and where individuals may direct privacy concerns or complaints. This information is publically available on CritiCall Ontario's website. This privacy policy and procedures states that the CritiCall Privacy Lead is the contact person to whom concerns or complaints may be directed and provides the name and/or title, mailing address and contact information. This privacy policy and procedures also outlines the manner in which and the format, either in writing or by telephone, in which privacy concerns or complaints may be directed to HHS/CritiCall. This privacy policy also indicates that individuals may make a complaint regarding compliance with the *Act* and its regulation to the IPC and provides the mailing address and contact information for the IPC. As per this privacy policy and procedures, this information is made publicly available on CritiCall Ontario's website.

This privacy policy and procedures outlines the process to be followed in receiving privacy complaints. This includes any documentation that must be completed, provided and/or executed by the individual making the privacy complaint; the agent(s) responsible for receiving the privacy complaint; the required content of the documentation, if any; and the nature of the information to be requested from the individual making the privacy complaint.

Upon receipt of a privacy complaint, the policy and procedures requires that a determination be made of whether or not the privacy complaint will be investigated. This privacy policy and procedures identifies the CritiCall Privacy Lead as being responsible for making this determination, the time frame within which this determination must be made and the process that must be followed and the criteria that must be used in making the determination, including any documentation that must be completed, provided and/or executed and the required content of the documentation.

In the event that it is determined that an investigation will not be undertaken, this privacy policy and procedures requires that a letter be provided to the individual making the privacy complaint acknowledging receipt of the privacy complaint; providing a response to the privacy complaint; advising that an investigation of the privacy complaint will not be undertaken; advising the individual that he or she may make a complaint to the IPC if there are reasonable grounds to believe that HHS/CritiCall has contravened or is about to contravene the *Act* or its regulation; and providing contact information for the IPC.

In the event that it is determined that an investigation will be undertaken, this privacy policy and procedures requires that a letter be provided to the individual making the privacy complaint acknowledging receipt of the privacy complaint within two (2) business days of receipt; advising that

an investigation of the privacy complaint will be undertaken; explaining the privacy complaint investigation procedure; indicating whether the individual will be contacted for further information concerning the privacy complaint; setting out the projected time frame for completion of the investigation; and identifying the nature of the documentation that will be provided to the individual following the investigation.

This privacy policy and procedures identifies the CritiCall Privacy Lead as being responsible for sending the above noted letters to the individuals making privacy complaints and requires that the letter be sent within two (2) business days of receipt.

Where an investigation of a privacy complaint will be undertaken, this privacy policy and procedures identifies the CritiCall Privacy Lead as being responsible for investigating the privacy complaint, the nature and scope of the investigation (i.e. document reviews, interviews, site visits, inspections) and the process that must be followed in investigating the privacy complaint. This includes a discussion of the documentation that must be completed, provided and/or executed in undertaking the investigation; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

This privacy policy and procedures provides that the CritiCall Privacy Lead and the CritiCall Security Lead have been delegated day-to-day authority to manage the privacy program and the security program.

The process for addressing the recommendations arising from the investigation of privacy complaints and the agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations and for monitoring and ensuring the implementation of the recommendations is also addressed in this privacy policy and procedures. This privacy policy and procedures also sets out the nature of the documentation that will be completed, provided and/or executed at the conclusion of the investigation of the privacy complaint, including the agent(s) responsible for completing, preparing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

This privacy policy and procedures addresses the manner and format in which the findings of the investigation of the privacy complaint, including recommendations arising from the investigation and the status of implementation of the recommendations, are communicated. This privacy policy and procedures indicates that the CritiCall Privacy Lead is responsible for communicating the findings of the investigation; the mechanism and format for communicating the findings of the investigation; the time frame within which the findings of the investigation must be communicated; and to whom the findings must be communicated, including the HHS Chief Executive Officer or the CritiCall Executive Director.

This privacy policy and procedures requires the individual making the privacy complaint to be notified, in writing, of the nature and findings of the investigation and of the measures taken, if any, in response to the privacy complaint. This privacy policy and procedures requires that the individual making the privacy complaint be advised that he or she may make a complaint to the IPC if there are reasonable grounds to believe that the *Act* or its regulation has been or is about to be contravened. The contact information for the IPC is also provided to the individual making a complaint. The CritiCall Privacy Lead is responsible for providing the written notification to the individual making the privacy complaint and the time frame within which the written notification must be provided.

This privacy policy and procedures also outlines whether any other person or organization must be notified of privacy complaints and the results of the investigation of privacy complaints, and if so, the manner by which, the format in which and the time frame within which the notification must be provided and the agent(s) responsible for providing the notification.

Further, this privacy policy and procedures requires that a log be maintained of privacy complaints and identifies the CritiCall Privacy Lead as being responsible for maintaining the log and for tracking whether the recommendations arising from the investigation of privacy complaints are addressed within the identified timelines. It further addresses where documentation related to the receipt, investigation, notification and remediation of privacy complaints will be retained and the agent(s) responsible for retaining this documentation.

This privacy policy and procedures requires that all HHS/CritiCall agents comply with this policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. This policy and procedures also stipulates that compliance will be audited in accordance with the *P-27 Policy and Procedures In Respect of Privacy Audits*, sets out the frequency with which the policy and procedures will be audited and identifies the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures. The relationship between this policy and its procedures and the *P-29 Policy and Procedures for Privacy Breach Management* is also addressed.

P32. LOG OF PRIVACY COMPLAINTS

HHS/CritiCall has implemented and maintains a log of all Privacy Complaints. The CritiCall Privacy Lead is responsible for maintaining and updating the log. This privacy policy and procedures requires the following particulars to be included in the log:

- The date that the privacy complaint was received and the nature of the privacy complaint;
- The determination as to whether or not the privacy complaint will be investigated and the date that the determination was made;
- The date that the individual making the complaint was advised:
    - That the complaint will not be investigated and was provided a response to the complaint; or
    - That the complaint will be investigated;
- The agent(s) responsible for conducting the investigation;
- The dates that the investigation was commenced and completed;
- The recommendations arising from the investigation;
- The agent(s) responsible for addressing each recommendation;
- The date each recommendation was or is expected to be addressed;
- The manner in which each recommendation was or is expected to be addressed; and
- The date that the individual making the privacy complaint was advised of the findings of the investigation and the measures taken, if any, in response to the privacy complaint.

P33. POLICY AND PROCEDURES FOR PRIVACY INQUIRIES

This privacy policy and procedures has been developed and implemented to address the process to be followed when receiving, documenting, tracking and responding to privacy inquiries. The definition of the term "privacy inquiry" is included in this policy and includes inquiries relating to the privacy policies, procedures and practices implemented by HHS/CritiCall for the CCIS and related to the compliance of HHS/CritiCall with the *Act* and its regulation.

This privacy policy outlines the information that must be communicated to the public relating to the manner in which, to whom and where individuals may direct privacy inquiries. This privacy policy and procedures requires the following information to be communicated to the public: the name and/or title, mailing address and contact information of the CritiCall Privacy Lead to whom privacy inquiries may be directed; information relating to the manner in which privacy inquiries may be directed to HHS/CritiCall, in writing or by telephone; and information as to where individuals may obtain further information about the privacy policies, procedures and practices implemented by HHS/CritiCall for the CCIS.

This policy and procedures further outlines the process to be followed in receiving and responding to privacy inquiries. This policy states that the CritiCall Privacy Lead is responsible for receiving and responding to privacy inquiries; outlines the documentation that must be completed, provided and/or executed; the required content of the documentation; and the format (in writing) and content of the response to the privacy inquiry. The CritiCall Privacy Lead and CritiCall Security Lead have been delegated day-to-day authority to manage the privacy program and the security program, respectively.

This privacy policy and procedures requires all HHS/CritiCall agents to comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of a breach. This privacy policy and procedures also stipulates that compliance will be audited in accordance with the *P-28 Policy and Procedures In Respect of Privacy Audits*, sets out that this policy and procedures shall be audited on an annual basis and identifies the CritiCall Privacy Lead as being responsible for conducting the audit and for ensuring compliance with the policy and its procedures. The relationship between this policy and its procedures and the *P-31 Policy and Procedures for Privacy Complaints* and the *P-29 Policy and Procedures for Privacy Breach Management* is also addressed.

PART 2 – SECURITY DOCUMENTATION

The following section focuses on HHS/CritiCall's security policies and procedures as they relate to the CCIS. As CritiCall operates the CCIS on behalf of HHS, the policies and procedures are, in some cases, specific to the environment and staff in place at CritiCall, where the day-to-day activities related to the CCIS take place. Overarching accountability continues to rest with the HHS Chief Executive Officer and all participating hospitals contributing PHI and data to the CCIS are required to enter into agreements with HHS for the collection of CCIS PHI and data.

S1: INFORMATION SECURITY POLICY

HHS/CritiCall has developed and implemented this information security policy and procedures in relation to PHI received by HHS/CritiCall for the CCIS. This policy and procedures requires a comprehensive information security program to be developed and implemented consisting of administrative, technical, and physical safeguards that are consistent with established industry standards and best practices. The information security program must effectively address any threats and risks identified, must be amenable to independent verification and must be consistent with established security frameworks and control objectives. This security policy and procedures outlines the duties and responsibilities of agents in respect of the information security program and in respect of implementation of the administrative, technical and physical safeguards are also addressed.

This security policy and procedures requires HHS/CritiCall to undertake comprehensive and organization-wide threat and risk assessments of all CCIS information security assets, including PHI, as well as appropriate project specific threat and risk assessments. It also establishes and documents a methodology for identifying, assessing and remediating threats and risks and for prioritizing all threats and risks identified for remedial action.

This security policy and procedures requires that all HHS/CritiCall agents and authorized hospital-based users accessing and using the services and/or information assets provided or managed by HHS/CritiCall must take steps that are reasonable in the circumstances to ensure that confidential information including PI and PHI is protected against theft, loss and unauthorized use or disclosure, and to ensure that the confidential records including PI and PHI are protected against unauthorized copying, modification or disposal.

This security policy and procedures outlines specific accountabilities and responsibilities for protection of confidential information in respect of the information security program are detailed in position descriptions of employees and are included in all agreements entered into by HHS/CritiCall.

This security policy and procedures states that the information security program shall:

- Engage and include the participation of stakeholders when appropriate;
- Guide and promote security strategy and security architecture, aligned with business objectives, strategy, and requirements;
- Develop appropriate organizational and individual awareness, motivation, and capability; and

- Report and make recommendations for action or improvement to the CritiCall Executive Council, the CritiCall Executive Director and the HHS CEO on security posture, security incidents, the status and effectiveness of the information security program.

This information security policy and procedures requires the security program to consist of the following objectives and security policies, procedures and practices:

- A security governance framework for the implementation of the information security program, including security training and awareness;
- The ongoing review of the security policies, procedures and practices implemented;
- Ensuring the physical security of the premises;
- The secure retention, transfer and disposal of records of personal health information, including policies and procedures related to mobile devices, remote access and security of PHI and data at rest;
- Establishing access control and authorization including business requirements, user access management, user responsibilities, network access control, operating system access control and application and information access control;
- Information systems acquisition, development and maintenance including the security requirements of information systems, correct processing in applications, cryptographic controls, security of system files, security in development and support procedures and technical vulnerability management;
- Monitoring, including policies and procedures, for maintaining and reviewing system control and security audit logs and security audits;
- Network security management, including patch management and change management;
- The acceptable use of information technology;
- Back-up and recovery;
- Information security breach management; and
- Establishing protection against malicious and mobile code.

The information security policies and procedures are established by the CritiCall Security Lead in consultation with key stakeholders and other business units/parties as appropriate. The policies and procedures shall be reviewed and approved by the CritiCall Executive Director. Subsequent to the review and approval by the CritiCall Executive Director, policies and procedures shall be reviewed by the HHS Chief Security Officer or delegate and approved by the HHS Chief Security Officer.

This information security policy and procedures outlines the information security infrastructure implemented by HHS/CritiCall including the transmission of PHI over authenticated, encrypted and secure connections; the establishment of hardened servers, firewalls, demilitarized zones and other perimeter defences; anti-virus, anti-spam and anti-spyware measures; intrusion detection and prevention systems; privacy and security enhancing technologies; and mandatory system-wide password-protected screen savers after a defined period of inactivity.

In addition, this information security policy and procedures requires a credible program to be implemented for continuous assessment and verification of the effectiveness of the security program in order to deal with threats and risks to CCIS data holdings containing PHI.

HHS/CritiCall requires all agents to comply with this policy and with all other security policies, procedures and practices implemented by HHS/CritiCall and addresses how and by whom compliance will be enforced and the consequences of a breach. In this regard, the information security policy stipulates that compliance will be audited in accordance with the *S-15 Policy and Procedures In Respect of Security Audits*, on an annual basis by the CritiCall Security Lead or delegate. The CritiCall Security Lead is also responsible for ensuring compliance with this policy.

This security policy requires all agents to notify HHS/CritiCall by way of the CCIS HelpDesk at the first reasonable opportunity, in accordance with the *S-17 Policy and Procedures for Information Security Breach Management*, if an agent breaches or suspects there may have been a breach of this policy or any of the security policies, procedures and practices implemented.

S2: POLICY AND PROCEDURES FOR ONGOING REVIEW OF SECURITY POLICIES, PROCEDURES AND PRACTICES

This security policy and associated procedures has been developed and implemented for the ongoing annual review of the security policies, procedures and practices. This security policy and procedures identifies the procedure to be followed in amending and/or drafting new security policies, procedures and practices if deemed necessary as a result of the annual review. The CritiCall Security Lead with support from the CritiCall Manager, Information Technology are responsible for developing CCIS Information Security policies, procedures and practices. These policies are reviewed on an annual basis, the purpose of which is to ensure all policies, procedures and practices are accurate and up-to-date, and if not, amendments will be made. The CritiCall Security Lead with support from the CritiCall Manager, Information Technology, is responsible for initiating, managing and documenting the completion of the annual review process. This security policy and procedures identifies the CritiCall Security Lead as being responsible for the procedure that must be followed in obtaining approval of any amended or newly developed security policies, procedures and practices.

This security policy and procedures states that in undertaking the review and determining whether amendments and/or new security policies, procedures and practices are necessary, HHS/CritiCall has regard to any orders, decisions guidelines, fact sheets and best practices issued by the IPC under the *Act* and its regulation; evolving industry security standards and best practices; technological advancements; amendments to the *Act* and its regulation relevant to HHS/CritiCall; and recommendations arising from privacy and security audits, privacy impact assessments, threat risk assessments (TRAs) and investigations into privacy complaints, privacy breaches and information security breaches. This security policy also takes into account whether the security policies, procedures and practices of HHS/CritiCall continue to be consistent with its actual practices and whether there is consistency between and among the security and privacy policies, procedures and practices implemented.

This security policy and procedures provides that the CritiCall Security Lead, in collaboration with the CritiCall Privacy Lead are responsible for amending any communication material in relation to the new or amended policies and procedures. This security policy and procedures outlines the method and nature of the communication. All entities and individuals involved in the operational planning and day-to-day activities of CCIS must be notified of all amendments made to the security policies, procedures and practices.

This security policy and procedures requires that all HHS/CritiCall agents comply with the policy and its procedures and identifies the CritiCall Security Lead as being responsible for compliance and enforcement of this policy and procedures, in addition to, addressing the consequences of a breach. This policy and procedures also stipulates that compliance will be audited in accordance with the *S-15 Policy and Procedures In Respect of Security Audits*, on an annual basis by the CritiCall Security Lead. The CritiCall Security Lead is also responsible for ensuring compliance with this policy and its procedures.

S3: POLICY AND PROCEDURES FOR ENSURING PHYSICAL SECURITY OF PERSONAL HELATH INFORMATION

This policy and procedures has been developed and implemented by HHS/CritiCall to ensure physical safeguards are implemented by CritiCall, third party service providers and other agents involved with the CCIS to: prevent unauthorized access to PHI; prevent accidental or intentional disclosure of PHI to unauthorized individuals; protect PHI against theft, loss and unauthorized use or disclosure of sensitive information residing on the hardware that is housed at CritiCall offices and the third party service provider data centre; and protect records of PHI against unauthorized copying, modification or disposal.

This policy and associated procedures addresses the physical safeguards implemented by HHS/CritiCall to protect PHI against theft, loss and unauthorized use or disclosure and to protect records of PHI against unauthorized copying, modification or disposal.

The physical safeguards implemented include controlled access to the premises and to locations within the premises where records of PHI are retained such as locked, alarmed, restricted and/or monitored access.

This security policy and procedures states that CritiCall Ontario's office be divided into varying levels of security with each successive level being more secure and restricted to fewer individuals. In order to access locations within the premises where records of PHI are retained, individuals are required to pass through multiple levels of security.

HHS/CritiCall requires all agents to comply with this policy and its procedures and identifies how the responsible party, the CritiCall Security Lead, will ensure compliance is enforced and the consequences of a breach. This policy and procedures also stipulates that compliance will be audited in accordance with the *S-15 Policy and Procedures In Respect of Security Audits*. The CritiCall Security Lead is responsible for conducting an audit and for ensuring compliance with this policy and procedures on an annual basis.

This policy and procedures requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the *S-17 Policy and Procedures for Information Security Breach Management*, if an agent breaches or suspects that there may have been a breach of this policy or its associated procedures.

Policy, Procedures and Practices with Respect to Access by Agents

This security policy and procedures details the various levels of access that may be granted to the

premises and to locations within the premises where records of PHI are retained.

This security policy and procedures states that the CritiCall Security Lead is responsible for receiving, reviewing, granting and terminating access by agents to the premises and to locations within the premises where records of PHI are retained, including the levels of access that may be granted. The process to be followed and the requirements that must be satisfied are also identified, including any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.

This security policy and procedures addresses the criteria that must be considered by the CritiCall Security Lead for approving and determining the appropriate level of access. The criteria is based on the "need to know" principle and ensures that access is only provided to agents who routinely require such access for their employment, contractual or other responsibilities. In the event that an agent only requires such access for a specified period, this policy and procedures has established a process for ensuring that access is permitted only for that specified period.

This security policy and procedures also sets out the manner in which the determination relating to access and the level of access is documented; to whom this determination will be communicated; any documentation that must be completed, provided and/or executed by the agent(s) responsible for making the determination; and the required content of the documentation.

This security policy and procedures identifies the CritiCall Security Lead as the responsible party and the process to be followed in providing identification cards, access cards and/or keys to the premises and to locations within the premises. This includes a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; and the required content of the documentation.

Theft, Loss and Misplacement of Identification Cards, Access Cards and Keys

This security policy and procedures requires agents to notify HHS/CritiCall at the first reasonable opportunity of the theft, loss or misplacement of identification cards, access cards and/or keys and sets out the process that must be followed in this regard. This security policy and procedures states that notification must be provided to the CCIS Help Desk; the nature and format of the notification, in writing or via telephone; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent to whom the documentation must be provided; and the required content of the documentation.

The CCIS Help Desk is responsible for all deactivation of identification and access cards and for the retrieval of keys. The following process must be followed upon theft, loss or misplacement of identification cards, access cards and keys of an agent in accordance with the *S17 - Policy and Procedures for Information Security Breach Management*:

- The loss (or theft) of identification cards, access cards and/or keys must be reported to the CCIS Help Desk by telephone as soon as the loss or theft is discovered or suspected. The CCIS Help Desk shall follow the procedures *S-17 Policy and Procedures for Information Security Breach Management;*

- The CCIS Help Desk shall de-activate the access card/and or keys as soon as possible;
- The CCIS Help Desk shall notify the CritiCall Executive Director and the CritiCall Security Lead, and record the loss or theft of identification cards, access cards and keys in the Security Breach Log to maintain a record of all reported lost or stolen keys and access cards; and
- The manager of the individual who has had the identification card, access card and/or keys stolen, misplaced or lost must also be notified.

The safeguards that are required to be implemented as a result of the theft, loss or misplacement of identification cards, access cards and/or keys are outlined in this security policy and procedures and identifies the CritiCall Security Lead as being responsible for implementing the safeguards.

This security policy and procedures also addresses the circumstances in which and the procedure that must be followed in issuing temporary or replacement identification cards, access cards and/or keys and the agent(s) responsible for issuing them. This includes a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent to whom the documentation must be provided; the required content of the documentation; the agent(s) to whom temporary identification cards, access cards and/or keys shall be returned; and the time frame for return.

This security policy and procedures outlines the process that must be followed by the CritiCall Security Lead in the event that temporary identification cards, access cards and/or keys are not returned. This policy and procedures also outlines the time-frame within which the process must be implemented.

Termination of the Employment, Contractual or Other Relationship

This policy and procedures requires agents, as well as their supervisors, to notify the hiring manager of the termination of their employment, contractual or other relationship with HHS/CritiCall and to return their identification cards, access cards and/or keys to the hiring manager on or before the date of termination of their employment, contractual or other relationship in accordance with *H10: Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship*.

This policy and procedures requires access to the premises to be terminated upon the cessation of the employment, contractual or other relationship in accordance with the *H-10 Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship.*

Notification When Access is No Longer Required

This security policy and procedures identifies the process that must be followed in providing notification, the method by which access will be terminated, and the time frame within which access must be terminated. This policy requires an agent, and their supervisor, who no longer requires access to the physical premises or to the area of the premises where records of PHI are retained, to notify the CritiCall Security Lead, in writing, in advance of the date that the access is no longer required or on the day that access is no longer required.

This security policy and procedures states that notification must include whether the individual no longer needs access to the area of the premises where records of PHI are retained or whether access

to all premises is no longer required and the date after which access is no longer required. The CritiCall Security Lead shall take the necessary steps to ensure that deactivation of access cards is arranged for the date when access is no longer required and shall document that the individual no longer has access to the secure premises once this is the case.

Audits of Agents with Access to the Premises

This security policy and procedures states that all agents must comply with this policy. The responsibility and accountability for compliance with this policy and procedures rests with the CritiCall Executive Director. Compliance with this policy and procedures will be audited in accordance with the *S15: Policy and Procedures In Respect of Security Audits.* The purpose of the audit is to ensure that agents granted access to the premises and to locations within the premises where records of PHI are retained continue to have an employment, contractual or other relationship with HHS/CritiCall and continue to require the same level of access.

A physical security audit of HHS/CritiCall's physical facility is conducted at least annually. The CritiCall Executive Director shall ensure that any third party service provider of facilities processing PHI conduct a quarterly audit of access to premises as per the agreement with the third party service provider. The third party service must provide a report, in writing, to the CritiCall Executive Director on completion of the audit.

A report of the physical security audit must be prepared for review by the CritiCall Executive Director and HHS Chief Security Officer following each security audit. The physical security audit report must describe each activity undertaken, when the activity was performed, by whom, the result of the audit (findings), and recommendations to correct any deficiencies identified. The findings of security audits shall be included in reports to the CritiCall Enterprise Risk Management Committee and to the HHS Chief Executive Officer.

Tracking and Retention of Documentation Related to Access to the Premises

This security policy and procedures requires that a log be maintained of agents granted approval to access the premises of HHS/CritiCall and to locations within the premises where records of PHI are retained and identifies the CritiCall Security Lead as being responsible for maintaining such a log. This policy and procedures also includes details related to where documentation related to the receipt, review, approval and termination of access to the premises and to locations within the premises where PHI is retained will be maintained and that the CritiCall Security Lead is responsible for maintaining this documentation.

Policy, Procedures and Practices with Respect to Access by Visitors

This security policy and procedures identifies the CritiCall Security Lead as being responsible and the process to be followed in identifying, screening and supervising visitors to the premises of HHS/CritiCall. This security policy and procedures sets out the identification that is required to be worn by visitors; any documentation that must be completed, provided and/or executed by agent(s) responsible for identifying, screening and supervising visitors; and the documentation that must be completed, provided and/or executed by visitors. Visitors are required to record their name, date and time of arrival, time of departure and the name of the agent(s) with whom the visitors are meeting.

This policy and procedures identifies the duties and responsibilities of the agents responsible for identifying, screening and supervising visitors. These duties include ensuring that visitors are accompanied at all times; ensuring that visitors are wearing the identification issued by HHS/CritiCall; ensuring that the identification is returned prior to departure; and ensuring that visitors complete the appropriate documentation upon arrival and departure. At the end of each day, the CritiCall Office Manager or delegate must review the visitor log and check that all visitors have signed out and returned their visitor pass.

If the CritiCall Office Manager or delegate finds that a visitor who has signed in, has not signed out and/or has not returned the visitor pass, the CritiCall Office Manager or delegate will notify the staff member who accompanied the visitor and the CritiCall Security Lead via e-mail that the visitor has not signed out and/or has not returned the visitor pass. The staff member shall be responsible for following up and documenting in the visitor log that the visitor was seen leaving the premises. The CritiCall Security Lead shall investigate any situation where a visitor has not been seen leaving the building and has not returned their visitor pass. The investigation will be conducted and documented as per *S17: Policy and Procedures for Information Security Breach Management.* This security policy and procedures also addresses where documentation related to the identification, screening and supervision of visitors will be retained and the agent(s) responsible for retaining this information.

S4: LOG OF AGENTS WITH ACCESS TO THE PREMISES OF THE PRESCRIBED PERSON OR PRESCRIBED ENTITY

HHS/CritiCall has implemented and maintains a log of agents who have been granted access to the premises of HHS/CritiCall. The CritiCall Security Lead is responsible for maintaining and updating this log. The log includes the following information for each agent that accesses the premises:

- Name of agent granted approval to access the premises;
- Level and nature of access granted;
- Locations within the premises that are accessible to the agent;
- Date access was granted;
- Date identification cards, access cards and/or keys were provided;
- The identification number on identification cards, access cards and/or keys, if any;
- Date of next audit of access;
- Date identification cards, access cards and/or keys were returned; and
- Date of access termination.

S5: POLICY AND PROCEDURES FOR SECURE RETENTION OF RECORDS OF PERSONAL HEALTH INFORMATION

This policy and procedures was created and implemented to identify the HHS/CritiCall agents responsible for ensuring the secure retention, transfer and retrieval of records of PHI and the precise methods by which records of PHI in paper and electronic format are to be securely retained in the CCIS.

This security policy and procedures provides a comprehensive schedule, which outlines the particular types of PHI and other records, format of the PHI and records, the authorized individual for ensuring secure retention and the retention period for the PHI and records. By way of summary, there are eight (8) types of information including: PHI in the CCIS, PHI on back-up tapes, PHI in core data export (electronic and hard copy), PHI for research (electronic and hard copy) and PHI shared through Data Sharing Agreements for non-research purposes (electronic and hard copy). For records of PHI used for research purposes, HHS/CritiCall must ensure that the records of PHI are not being retained for a period longer than that set out in the written research plan approved by a research ethics board. For records of PHI collected pursuant to a Data Sharing Agreement, this policy and procedures prohibits the records from being retained for a period longer than that set out in the Data Sharing Agreement. This policy and procedures requires that records of PHI be retained for only as long as necessary to fulfill the purposes for which the PHI was collected.

This security policy and procedures requires records of PHI to be retained in a secure manner and identifies the CritiCall Security Lead as being responsible for ensuring the secure retention of these records. This policy and procedures identifies the precise methods by which records of PHI in paper and electronic format are to be securely retained, including records retained in various media.

This security policy and procedures states that agents of HHS/CritiCall, who have CCIS-related duties that require them to record, access, view or work with PHI, must take steps that are reasonable in the circumstances to ensure that PHI is protected against theft, loss and unauthorized use or disclosure and that records of PHI are protected against unauthorized copying, modification or disposal. This shall include but is not limited to:

- Electronic media shall be stored in a secure location and protected from unauthorized access;
- Electronic media shall be safeguarded with the administrative, technical and physical controls;
- Access to PHI must be restricted to authorized individuals who need to access PHI to perform their day-to-day activities;
- Media containing PHI shall be encrypted with a minimum of 128-bit Advanced Encrypted Standard (AES) level;
- Media containing PHI must be password protected in accordance with *S9: Policy and Procedures Related to Passwords*;
- Paper records shall be stored in a secure locked area; and
- Access to PHI records shall be limited to agents of HHS/CritiCall with an appropriate level of access controls based on their roles and responsibilities.

This security policy and procedures states that if a third party service provider is contracted to retain records of PHI on behalf of HHS/CritiCall, a written agreement that contains the relevant language from the *P20: Template Agreement For All Third Party Service Providers* must be executed with the third party prior to transferring any PHI, and include:

- The purposes for which records of PHI will be transferred to the third party service provider for secure retention must be documented;
- The procedures to be followed in securely transferring the records of PHI to the third party service provider and in securely retrieving the records from the third party service provider, including the secure manner in which the records will be transferred and retrieved, the conditions pursuant to which the records of PHI will be transferred and retrieved and the agent(s) responsible for ensuring the secure transfer and retrieval of the records of PHI. In this regard, the policy and procedures shall comply with the *S7: Policy and Procedures for Secure Transfer of Records of Personal Health Information*;
- Documentation that is required to be maintained in relation to the transfer of records of PHI to the third party service provider for secure retention;
- Identifies the CritiCall Security Lead as being responsible for ensuring the secure transfer of records of PHI and to document the date, time and mode of transfer and maintain a repository if written confirmations received from the third party service provider upon receipt of the records of PHI;
- The requirement that the third party service provider who identifies a suspected or actual breach of privacy or security report the incident to the CCIS Help Desk as soon as possible in accordance with *P29 - Policy and Procedures for Privacy Breach Management* and *S17-Policy and Procedures for Information Security Breach Management.*

This policy and procedures also requires a detailed inventory to be maintained of records of PHI being securely retained by the third party service provider and of records of PHI retrieved by HHS/CritiCall and identifies the CritiCall Security Lead as being responsible for maintaining the detailed inventory.

If a third party service provider is contracted to retain records of PHI, this policy and procedures requires that a written agreement be executed with the third party service provider containing the relevant language from the *P-20 Template Agreement For All Third Party Service Providers*, and identifies the CritiCall Executive Director as responsible for ensuring that the agreement has been executed prior to transferring the records of PHI for secure retention.

This security policy and procedure requires all HHS/CritiCall agents to comply with this policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of a breach. This policy and procedures also stipulates that compliance will be audited, on an annual basis, in accordance with the *S-15 Policy and Procedures In Respect of Security Audits* by the CritiCall Security Lead. The CritiCall Security Lead is responsible for conducting the audit and for ensuring compliance with this policy and its procedures.

This policy and procedures requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the *S-17 Policy and Procedures for Information Security Breach Management*, if an agent breaches or suspects there may have been a breach of this policy or its procedures.

S6: POLICY AND PROCEDURES FOR SECURE RETENTION OF RECORDS OF PERSONAL HEALTH INFORMATION ON MOBILE DEVICES

HHS/CritiCall has developed and implemented a policy and procedures to address whether and in what circumstances PHI is permitted to be retained on mobile device. For the purposes of this policy and procedures 'mobile device' is defined as any portable computing device that can be used to store, retrieve, manipulate, and transmit data, which includes but is not limited to: USB keys, jump drives, memory keys, laptops, notebooks, tablets, PDAs, and smart phones.

In drafting this policy HHS/CritiCall had regard to Orders issued by the IPC including Order HO-004 and Order HO-007; and with guidelines, fact sheets and best practices issued by the IPC pursuant to *PHIPA* and its Regulation, including *Fact Sheet 12: Encrypting Personal Health Information on Mobile Devices, Fact Sheet 14: Wireless Communication Technologies: Safeguarding Privacy and Security and Safeguarding Privacy in a Mobile Workplace*

It is the responsibility of HHS/CritiCall to provide direction to all agents that support the ongoing operation, management and maintenance of the CCIS to:

- Prevent unauthorized access to Personal Health Information (PHI) on mobile devices;
- Prevent unauthorized access to PHI by remote access; and
- Protect PHI on mobile devices against theft, loss, unauthorized use or disclosure and unauthorized copying, modification or disposal.

This security policy and procedures states that HHS/CritiCall requires all agents to comply with this policy and its procedures and addresses how the CritiCall Security Lead will ensure compliance will be enforced and the consequences of a breach. This policy and procedures also stipulates that compliance will be audited in accordance with the *S-15 Policy and Procedures In Respect of Security Audits*, on an annual basis. This policy and procedures states that the CritiCall Security Lead is responsible for conducting the audit and for ensuring compliance with this policy and its procedures.

This security policy and procedures require agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the *S-17 Policy and Procedures for Information Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.

Where Personal Health Information is Permitted to be Retained on a Mobile Device

HHS/CritiCall's policy and procedure requires that all mobile devices used to retain CCIS PHI will be encrypted and enabled with password protection in accordance with the *S-9 Policy and Procedures Relating to Passwords* and in consideration of the *IPC Fact Sheet 12: Encrypting Personal Health Information on Mobile Devices.* This policy also sets out the circumstances in which retention of PHI on a mobile device is permitted.

Approval Process for Retention of PHI on a Mobile Device

This policy and procedures states that approval is required prior to retaining PHI on a mobile device. The policy and procedures includes a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation. In circumstances where PHI is required to be retained on mobile devices, a request must be submitted in writing to the CritiCall Security Lead who is responsible for receiving, reviewing and determining whether to approve or deny a request for the retention of PHI on a mobile device. Prior to retaining PHI on a mobile device, the requesting party must provide the following particulars to the CritiCall Security Lead

- Name of the requester;
- The nature of the PHI being retained;
- The reason for retaining PHI on a mobile device;
- Date, time and duration for the retention of PHI;
- Type of device used for retention of PHI; and
- The method of removing PHI from the mobile device.

This policy and procedures states that the CritiCall Security Lead shall review the request and make a recommendation whether to approve or deny the request for the retention of PHI on a mobile device. In determining whether to recommend the approval or denial of the request the CritiCall Security Lead shall consider:

- The reason for the request;
- The type of device that is being proposed; and
- The proposed method for removing PHI from the device.

This security policy and procedures states that prior to any approval of a request to retain PHI on a mobile device, the CritiCall Security Lead shall ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose and that no more PHI will be retained on the mobile device than is reasonably necessary to meet the identified purpose. The CritiCall Security Lead shall ensure that, when determining whether to recommend the approval or denial of the request, the use of PHI is consistent with the *P8 - Policy and Procedures for Limiting Agent Access to Personal Health Information.*

If, in the opinion of the CritiCall Security Lead, the request is reasonable and all the conditions have been met, the CritiCall Security Lead shall recommend that the CritiCall Executive Director, approve the request. The CritiCall Executive Director shall review the recommendation and approve or deny the request. The decision of the CritiCall Executive Director shall be communicated to the requestor, in writing, including the reason for the approval or denial.

Conditions or Restrictions on the Retention of Personal Health Information on a Mobile Device

This security policy and procedures requires the CritiCall Security Lead to ensure that the mobile devices containing PHI are encrypted as well as password-protected using strong and complex

passwords that are in compliance with the *S9 - Policy and Procedures Relating to Passwords*. This policy and procedures requires that mobile devices have a display screen, equipped with a mandatory standardized password-protected screen saver that must be enabled after 15 minutes of inactivity also in accordance with *S9 - Policy and Procedures Relating to Passwords*. The CritiCall Security Lead is responsible for encrypting mobile devices and for ensuring that mandatory standardized password-protected screen saver is enabled.

This policy and procedures requires all HHS/CritiCall agents who are granted approval to retain PHI on a mobile device, to comply with this policy. At a minimum, the HHS/CritiCall agents retaining PHI on mobile devices must:

- Be prohibited from retaining PHI on a mobile device if other information, such as de-identified and/or aggregate information, will serve the purpose;
- De-identify the PHI to the fullest extent possible;
- Be prohibited from retaining more PHI on a mobile device than is reasonably necessary for the identified purpose;
- Be prohibited from retaining PHI on a mobile device for longer than necessary to meet the identified purpose; and
- Ensure that the strong and complex password for the mobile device is different from the strong and complex passwords for the files containing the PHI and that the password is supported by "defence in depth" measures.

This policy and procedures details the steps that must be taken by agents to protect the PHI retained on a mobile device against theft, loss and unauthorized use or disclosure and to protect the records of PHI retained on a mobile device against unauthorized copying, modification or disposal.

This policy and procedures also requires agents of HHS/CritiCall to retain the PHI on a mobile device in compliance with the *S5 - Policy and Procedures for Secure Retention of Records of Personal Health Information* and to securely delete PHI retained on a mobile device in accordance with the process and in compliance with the time-frame outlined in this policy and procedures.

Where Personal Health Information is not Permitted to be Retained on a Mobile Device

This security policy and procedure states that where PHI is prohibited to be retained on mobile devices, permission for remote access to PHI through a secure connection or virtual private network, may be permitted with the prior approval of the CritiCall Executive Director using the following approval process.

Approval Process for Accessing PHI Remotely

This security policy and procedures includes a discussion of the process that must be followed and the HHS/CritiCall agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for remote access to PHI; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation. The CritiCall Security Lead is responsible for receiving, reviewing, and determining whether to approve or deny the request for remote access to PHI. This policy and

procedures requires that the agent requesting remote access to PHI must provide the following information, in writing, to the CritiCall Security Lead:

- Name of the requestor;
- The reason for accessing PHI remotely;
- Date and time for the access to PHI;
- Type of device to be used for remotely accessing PHI;
- How the PHI will be protected in transit; and
- The method of removing PHI from the device used to access.
-

The CritiCall Security Lead, in collaboration with the Manager, Information Technology, shall ensure that a virtual private network (VPN) or secure communication channel is established between user and system configured for remote access. The following precautions shall be implemented to protect the system containing PHI:

- Remote access shall only be provided via a software/hardware VPN solution;
- VPN access shall require authentication of an account/password combination;
- Account/password shall be unique and traceable to an individual; and
- User account name and password shall comply with *S9 - Policy and Procedures Relating to Passwords.*

This security policy and procedures requires that prior to any approval of a remote access to PHI, the CritiCall Security Lead must determine whether to make a recommendation to approve or deny the request, and will ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose and that no more PHI will be accessed than is reasonably necessary to meet the identified purpose. This policy and procedures states that in coming to a decision on whether to approve remote access to PHI, the CritiCall Security Lead shall ensure that the use of PHI has been approved pursuant to the *P8 - Policy and Procedures for Limiting Agent Access to Personal Health Information.*

If, in the opinion of the CritiCall Security Lead, the request is reasonable and all the conditions have been met, the CritiCall Security Lead shall recommend that the CritiCall Executive Director, approve the request. The CritiCall Executive Director shall review the recommendation and approve or deny the request. The decision shall be communicated by the CritiCall Security Lead to the requestor, in writing, including the reason for denial, if the request has been denied.

This security policy and procedures requires the CritiCall Security Lead to maintain a log for individuals who are granted permission to access PHI remotely.

Conditions or Restrictions on the Remote Access to Personal Health Information

This policy and procedures identifies the conditions or restrictions with which HHS/CritiCall agents granted approval to access PHI remotely must comply. All HHS/CritiCall agents must be prohibited from remotely accessing PHI if other information, such as de-identified and/or aggregate information, will serve the purpose and from remotely accessing more PHI than is reasonably

necessary for the identified purpose. This policy and procedures also sets out the administrative, technical and physical safeguards that must be implemented by agents in remotely accessing PHI.

S7: POLICY AND PROCEDURES FOR SECURE TRANSFER OF RECORDS OF PERSONAL HEALTH INFORMATION

HHS/CritiCall has developed and implemented this policy and procedures with respect to the secure transfer of records of PHI in paper and electronic format.

This policy and procedures requires records of PHI to be transferred in a secure manner and sets out the secure methods of transferring records of PHI in paper and electronic format that have been approved by HHS/CritiCall. The policy and procedures require HHS/CritiCall agents to use the approved methods of transferring records of PHI and prohibits all other methods.

This security policy and procedures requires that the processes outlined must be followed in transferring records of PHI through each of the approved methods must also be followed. This includes a discussion of the conditions pursuant to which records of PHI will be transferred; the HHS/CritiCall agent(s) responsible for ensuring the secure transfer; any documentation that is required to be completed, provided and/or executed in relation to the secure transfer; the HHS/CritiCall agent(s) responsible for completing, providing and/or executing the documentation; and the required content of the documentation.

This security policy and procedures states that the CritiCall Security Lead is responsible for transferring records of PHI and is required to document the date, time and mode of transfer; the recipient of the records of PHI; and the nature of the records of PHI transferred. Further, this policy and procedures requires the recipient to confirm receipt of the records of PHI, in addition to, identifying the CritiCall Security Lead as being responsible for noting the manner of obtaining and recording acknowledgement of receipt of the records of PHI.

This security policy and procedures outlines the administrative, technical and physical safeguards that must be implemented by HHS/CritiCall agents prior to transferring records of PHI through each of the approved methods to ensure that the records of PHI are transferred in a secure manner.

HHS/CritiCall is responsible for ensuring that the approved methods of securely transferring records of PHI and the procedures and safeguards that are required to be implemented in respect of the secure transfer of records of PHI are consistent with:

- Orders issued by the IPC under the *Act* and its regulation, including but not limited to Order HO-004 and Order HO-007;
- Guidelines, fact sheets and best practices issued by the IPC, including Privacy Protection Principles for Electronic Mail Systems and Guidelines on Facsimile Transmission Security; and
- Evolving privacy and security standards and best practices.

HHS/CritiCall requires agents to comply with this policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of a breach. This policy and procedures also stipulates that compliance will be audited in accordance with the S15 - *Policy and Procedures*

In Respect of Security Audits, on an annual basis, by the CritiCall Security Lead who is responsible for conducting the auditing and for ensuring compliance with this policy and its procedures.

This security policy and procedures also requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the S17 - *Policy and Procedures for Information Security Breach Management*, if an agent breaches or suspects there may have been a breach of this policy or its procedures.

S8: POLICY AND PROCEDURES FOR SECURE DISPOSAL OF RECORDS OF PERSONAL HEALTH INFORMATION

HHS/CritiCall has developed and implemented a policy and procedures with respect to the secure disposal of records of PHI in both paper and electronic format in order to ensure that reconstruction of these records is not reasonably foreseeable in the circumstances.

This security policy and procedures requires records of PHI to be disposed of in a secure manner and provides a definition of 'secure disposal' that is consistent with the *Act* and its regulation. This policy and procedures further identifies the precise method by which records of PHI in paper format are required to be securely disposed of and the precise method by which records of PHI in electronic format, including records retained on various media, are required to be securely disposed of.

This security policy and procedures states that all records containing PHI (paper or electronic format) are to be disposed of or destroyed shall be disposed of or destroyed using secure methods consistent with *PHIPA* and its Regulation; with Orders issued by the IPC pursuant to *PHIPA* and its Regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the IPC pursuant to *PHIPA* and its Regulation, including *Fact Sheet 10: Secure Destruction of Personal Health Information.*

This security policy and procedures addresses the secure retention of records of PHI pending their secure disposal in accordance with the S5 - *Policy and Procedures for Secure Retention of Records of Personal Health Information.* This security policy and procedures states that paper documentation containing PHI must not be disposed of in waste baskets, recycling bins, or any other normal disposal methods. The CritiCall Privacy Lead is responsible for the secure physical storage location for paper records containing PHI pending disposal. PHI records, pending their secure disposal, shall be segregated from recycling material, clearly marked as awaiting secure disposal and locked in a secure location. Secure physical storage locations for decommissioned PHI records shall have appropriate safeguards in place in accordance with the *S6 - Policy and Procedures for Secure Retention of Records of Personal Health Information.*

This security policy and procedures states that in the event that records of PHI or certain categories of records of PHI are securely disposed of by a designated agent, who is not a third party service provider, the CritiCall Privacy Lead is responsible for securely disposing of the records of PHI; the responsibilities of the CritiCall Privacy Lead in securely disposing of the records; and the time frame within which, the circumstances in which and the conditions pursuant to which the records of PHI are securely disposed of is included. This policy and procedures also requires the CritiCall Privacy Lead to provide a certificate of destruction which includes the following information:

- Identifying the records of personal health information to be securely disposed of;
- Confirming the secure disposal of the records of personal health information;
- Setting out the date, time and method of secure disposal employed; and
- Bearing the name and signature of the agent(s) who performed the secure disposal.

This security policy and procedures states that the certificate of destruction must be provided to the CritiCall Privacy Lead within two (2) business days following the secure disposal of the records of PHI.

This security policy and procedures identifies the CritiCall, Manager of IT as being responsible for the secure disposal of electronic media containing PHI and must be disposed of by rendering the media unusable and discarding the media. HHS/CritiCall follows industry best practice for secure destruction. Non-magnetic media such as CDs and DVDs, must be securely stored physically up to six months for bulk secure destruction and disposal. Only designated HHS/CritiCall agents shall be authorized to access the secure storage location to receive, store and release media for disposal. If media such as hard drives and backup tapes are to be rendered unusable and discarded, they must be degaussed within a reasonable timeframe of removal from the original equipment. Decommissioned electronic media containing PHI shall be degaussed before leaving the CritiCall premises.

This security policy and procedures outlines the procedure to be followed by HHS/CritiCall when a third party service provider is retained for secure disposal. When the arrangements have been made for the secure destruction, the CritiCall Manager of IT or delegate shall retrieve the media and shall, if a hard drive, degauss the hard drive using industry best practice. The CritiCall Manger of IT or delegate shall ensure that decommissioned electronic media with serial numbers are recorded in a log by the serial number and type of IT hardware it originated from (i.e., server), and that decommissioning media without serial number (i.e., CD or DVD) will be logged with any identifying marking on the media, originating source and date remitted for disposal. The electronic media decommissioning log must be retained by the delegated personnel for at least seven years.

This security policy and procedures outlines the procedure that must be followed by HHS/CritiCall agents when securely transferring the records of PHI to a third party service provider for secure disposal. This security policy and procedures identifies the secure manner in which the records of PHI will be transferred to the third party service provider, the conditions pursuant to which the records will be transferred and states that the CritiCall, Privacy Lead or delegate is responsible for ensuring the secure transfer of the records. This policy and procedures complies with the S7 - *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.

This security policy and procedures states that the CritiCall Privacy Lead is responsible for ensuring the secure transfer of records of PHI and must document the date, time and mode of transfer of the records of PHI and to maintain a repository of written confirmations received from the third party service provider evidencing receipt of the records of PHI. A detailed inventory related to the records of PHI transferred to the third party service provider for secure disposal is also maintained and the policy and procedures identifies the CritiCall, Manager IT as being responsible for maintaining this inventory.

When a third party service provider is retained to securely dispose of records of PHI, the policy and procedures requires that a written agreement be executed with the third party service provider containing the relevant language from the P20 - *Template Agreement For All Third Party Service Providers*, and identifies the CritiCall Privacy Lead as being responsible for ensuring that the agreement has been executed prior to the transfer of records of PHI for secure disposal.

This policy and procedures outlines the procedure to be followed in tracking the dates that records of PHI are transferred for secure disposal and the dates that certificates of destruction are received, and whether from the third party service provider or from the designated HHS/CritiCall agent that is not a third party service provider. The CritiCall Privacy Lead is responsible for conducting such tracking. This security policy and procedures outlines the process to be followed where a certificate of destruction is not received. If the certificate of destruction is not received within one (1) week from the date of destroying the records of PHI, the CritiCall Security Lead shall contact the third party to follow-up. If the third party service provider does not provide the certificate within two (2) business days following the contact, the CritiCall Security Lead shall notify both the CritiCall Privacy Lead and the CritiCall Executive Director who will meet to determine the most appropriate next steps. This policy and procedures requires the certificate of destruction to be stored in a secure location.

This security policy and procedures requires that all HHS/CritiCall agents comply with this policy and its procedures and identifies the CritiCall Security Lead as being the responsible party for enforcing compliance with this policy and procedures. This security policy and procedures states that compliance will be audited in accordance with the S15 - *Policy and Procedures In Respect of Security Audits* on an annual basis by the CritiCall Security Lead.

This security policy and procedures also requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the S17 - *Policy and Procedures for Information Security Breach Management*, if an agent breaches or suspects there may have been a breach of this policy or its procedures.

This security policy and procedures identifies that if a breach of this policy is found to have occurred, an investigation will be conducted by the CritiCall Security Lead. The policy and procedures also identifies that where a breach is found to be intentional or the result of continuous negligent work practices, disciplinary action will be taken up to and including termination of employment and/or laying criminal charges, as per *H11: Policy and Procedures for Discipline and Corrective Action.*

S9: POLICY AND PROCEDURES RELATING TO PASSWORDS

HHS/CritiCall has developed and implemented this security policy and procedures with respect to passwords. This policy and procedures sets out the requirements with respect to passwords for authentication and passwords for access to information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by HHS/CritiCall.

This security policy and procedures identifies the minimum password requirements which must be followed for systems and applications supported by HHS/CritiCall. Passwords must be kept confidential and satisfy the following requirements:

- Must be a minimum length of eight (8) characters;
- Must contain characters from the following four categories:
  - password must have at least one uppercase character (A — Z);
  - password must have at least one lowercase character (a — z);
  - password must have at least on numeric digit (0 — 9); and
  - password must have at least one non-alphanumeric values (For example: !, $, #, or %).

This security policy and procedures further identifies the administrative, technical and physical safeguards that must be implemented by agents in respect of passwords in order to ensure that the PHI is protected against theft, loss and unauthorized use or disclosure and that the records of PHI are protected against unauthorized copying, modification or disposal including the following:

- Users must not reuse the last three (3) passwords used;
- Passwords must be changed at a minimum, every 90 days;
- Passwords must be set to expire automatically every 90 days;
- Users must keep their password private and secure and must change their passwords immediately if they suspect that their password has become known to any other individual, including another agent;
- The CCIS user account must be automatically locked after five (5) unsuccessful login attempts;
- HHS/CritiCall workstations used for accessing the CCIS must be locked after 15 minutes of inactivity;
- The CCIS user password must be changed immediately if compromised or suspected to have become known to others;
- Upon suspicion or notice that a CCIS user password has been compromised, the CCIS user or the person who became aware of the suspected compromise, must report the compromise to the CCIS Helpdesk immediately; and
- The CCIS user password must not be written down, displayed, revealed, hinted at, shared or otherwise be made known to others.

HHS/CritiCall administers passwords for CCIS systems and applications. HHS/CritiCall is responsible for managing and maintaining two sets of user profiles (internal HHS/CritiCall user profiles and hospital-based user profiles).

The CritiCall Security Lead is responsible for ensuring that the password policy and procedures are updated as required and consistent with any orders and decisions issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation; with any guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario; and with evolving privacy and security standards and best practices

This security policy and procedures requires all HHS/CritiCall agents to comply with this policy and its procedures and identifies the CritiCall Security Lead as being responsible for ensuring compliance will be enforced and the consequences of a breach. This policy and procedures stipulates that compliance will be audited in accordance with the S15 - *Policy and Procedures In Respect of Security Audits*, on an annual basis by the CritiCall Security Lead. The CritiCall Security Lead will conduct a TRA and Penetration test every two years through an approved third party

service provider. The findings will be presented to the CritiCall Executive Committee and the HHS CISO in an executive summary format. Each mitigation task will be managed by the CritiCall Security Lead and signed off by the HHS CISO. Each risk and mitigation will be maintained by the CritiCall Security Lead in a Risk Registry.

This security policy and procedures requires all HHS/CritiCall agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the *Policy and Procedures for Information Security Breach Management*, if an agent breaches or suspects there may have been a breach of this policy or its procedures.

S10: POLICY AND PROCEDURES FOR MAINTAINING AND REVIEWING SYSTEM CONTROL AND AUDIT LOGS

HHS/CritiCall has developed and implemented this policy and procedures for the creation, maintenance and ongoing review of system control and audit logs that are consistent with evolving industry standards and that are commensurate with the amount and sensitivity of the PHI maintained, with the number and nature of HHS/CritiCall agents with access to PHI and with the threats and risks associated with the PHI.

This security policy and procedures requires HHS/CritiCall to ensure that all information systems, technologies, applications and programs involving PHI for the CCIS have the functionality to log access, use, modification and disclosure of PHI.

The purpose of this policy and procedures is to provide HHS/CritiCall employees, contracted workers and any other agents of HHS/CritiCall with the direction required to ensure system control and audit logs and practices are:

- Created, maintained and regularly reviewed;
- Consistent with *PHIPA*, its Regulation and the Manual;
- Consistent with evolving industry standards such as ISO 27001 & 27002;
- Adequate for the amount and sensitivity of PHI maintained; with the number and nature of agents with access to PHI; and with the threats and risks associated with the PHI;
- Ensure the ongoing methods for system monitoring and logging will allow for the timely detection of and response to unauthorized information processing activities; and
- All information systems, technologies, applications and programs involving PHI have the functionality to log access, use, modification and disclosure PHI.

This security policy and procedures sets out the types of events that must be audited and the nature and scope of the information that must be contained in system control and audit logs. This security policy and procedures requires the system control and audit logs to set out the date and time that PHI is accessed; the date and time of the disconnection; the nature of the disconnection; the name of the user accessing PHI; the network name or identification of the computer through which the connection is made; and the operations or actions that create, amend, delete or retrieve PHI including the nature of the operation or action, the date and time of the operation or action, the name of the user that performed the action or operation and the changes to values, if any.

The CritiCall Security Lead, in consultation with the HHS CSO, is responsible for:

- Setting out the types of events that will be required to be audited and ensuring that the audit occurs;
- Setting the schedule of audits on an annual basis and reviewing the audit schedule with the CritiCall Executive Director and ; and
- That the nature and scope of the information that is required to be contained in system control and audit logs is documented.

This security policy and procedures requires the system control and audit logs to be immutable, which means that HHS/CritiCall is required to ensure that the system control and audit logs cannot be accessed by unauthorized persons or amended or deleted in any way. This security policy and procedures sets out the procedures that must be implemented in this regard and identifies the CritiCall Security Lead as being responsible for implementing these procedures.

The CritiCall Security Lead shall ensure that the system control and audit logs are retained for two (2) years and shall be located in a secure location of the CritiCall document repository protected with administrative, technical and physical controls

The CritiCall Security Lead shall, according to the established schedule, send a request to the appropriate individual to run the system control and audit log report. Once the audit log report is completed it shall be forwarded to the CritiCall Security Lead. The CritiCall Security Lead is responsible for reviewing the log, documenting, and tracking the findings identified in the report and shall review the logs on a monthly basis and log the information into *S16: Log of Security Audits*. The CritiCall Executive Director is responsible for ensuring that audits are conducted by the CritiCall Security Lead as indicated.

This security policy and procedures states that the findings arising from the review of system control and audit logs must be documented. The CritiCall Security Lead is responsible for assigning other agent(s) to address the findings, for establishing timelines to address the findings, for addressing the findings and for monitoring and ensuring that the findings have been addressed.

This security policy and procedures sets out the nature of the documentation that must be completed, provided and/or executed following the review of system control and audit logs. This policy and procedures states that the CritiCall Security Lead is responsible for completing, providing and/or executing the required documentation; identifies the agent(s) to whom the documentation must be provided; the time frame within which the documentation must be provided; and the required content of the documentation.

This policy and procedures outlines the manner and format for communicating the findings of the review and how the findings have been or are being addressed. The CritiCall Security Lead shall communicate the findings of the review to the CritiCall Executive Director via monthly status update meetings or more frequently based on urgency of the findings. If a finding results in the identification of a privacy or security breach or a suspected privacy or security breach then the CritiCall Security Lead, will at the first reasonable opportunity initiate breach management activities in accordance with *P29 - Policy and Procedures for Privacy Breach Management* and *S17-Policy and Procedures for Information Security Breach Management.* The relationship between this policy and its procedures and the *P29 - Policy and Procedures for Privacy Breach Management* and the *Policy and Procedures for Information Security Breach Management* is also identified.

This security policy and procedures requires all HHS/CritiCall agents to comply with this policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of a breach. This security policy and procedures also stipulates that compliance will be audited in accordance with the S15 - *Policy and Procedures In Respect of Security Audits*, on an annual basis by the CritiCall Security Lead. The CritiCall Security Lead is responsible for ensuring compliance with this policy and its procedures.

This policy and procedures requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the S17 - *Policy and Procedures for Information Security Breach Management*, if an agent breaches or suspects there may have been a breach of this policy or its procedures.

S11: POLICY AND PROCEDURES FOR PATCH MANAGEMENT

HHS/CritiCall has developed and implemented a policy and procedures for patch management. This policy and procedures sets out the minimum requirements for patch management related activities; and documents the responsibilities of HHS/CritiCall employees and any other agents for: monitoring the availability of patches; determining the applicability of the patches to the HHS/CritiCall CCIS system and whether and when patches must be implemented; implementing patches; managing patches; and documenting the actions taken with respect to decision making and applying any patches.

The CritiCall Manager, IT, is accountable for the daily monitoring of patch availability. The patch management process includes an analysis of the available patches for verification of the source and integrity and include determining the impact of changes to the HHS/CritiCall environment prior to recommendation of implementation of the patches in the production environment. This policy and procedures discusses the criteria that must be considered by the Manager, Information Technology when undertaking an analysis regarding whether or not to implement a patch.

This security policy and procedures requires delegated HHS/CritiCall agents including third party service providers to perform regular non-intrusive scanning (vulnerability scan) of the systems and network to identify missing patches. A report shall be forwarded to the CritiCall Manager, IT or delegate indicating the environmental status of system patches.

The Manager, IT must assign a 'Patch Management Delegate' for each system. The Manager, Information Technology is accountable for notifying the appropriate 'Patch Management Delegate' of the availability of a patch and for describing the nature of the available patch.

In circumstances where a determination is made that the patch should not be implemented, this policy and procedures requires the CritiCall Manager, IT to document the description of the patch; the date that the patch became available; the severity level of the patch; the information system, technology, equipment, resource, application or program to which the patch relates; and the rationale for the determination that the patch should not be implemented.

If it is determined that a patch will be implemented the Patch Management Delegate shall:

- Determine the time frame within which the patch should be implemented according to the patch level criteria (as set out under Procedures) and the priority of the patch;
- The process by which these determinations are to be made and the documentation that must be completed, provided and/or executed in this regard; and
- Submit a change request according to the HHS/CritiCall change management process as set out in *S12 - Policy and Procedures Related to Change Management.*

This security policy and procedures also sets out the process for patch implementation, including the agent(s) responsible for patch implementation and any documentation that must be completed, provided and/or executed by the agent(s) responsible for patch implementation.

The circumstances in which patches must be tested, the time frame within which patches must be tested, the procedure for testing and the agent(s) responsible for testing is also addressed, including the documentation that must be completed, provided and/or executed by the agent(s) responsible for testing.

This security policy and procedures requires that the application of all patches to be applied must be fully documented in the HHS/CritiCall Patch Management Log by the Patch Management Delegate including:

- A description of the patch;
- The date the patch became available;
- The severity level and priority of the patch;
- The information system, technology, equipment, resource, application or program to which the patch relates;
- The date the patch was implemented;
- The date when the patch was tested, if any;
- The agent responsible for testing;
- Whether or not the testing was successful; and
- The agent(s) responsible for implementing the patch.

This security policy and procedures further sets out the criteria upon which determinations are to be made in circumstances where a determination has been made that a patch should not be implemented and the related documentation that must be completed.

This security policy and procedures requires agents to comply with the policy and its procedures and addresses how compliance will be enforced by the CritiCall Security Lead and the consequences of a breach. This policy and procedures also stipulates that compliance will be audited in accordance with the S15 - *Policy and Procedures In Respect of Security Audits*, on an annual basis by the CritiCall Security Lead. The CritiCall Security Lead is responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

This security policy and procedures also requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the S17 - *Policy and Procedures for Information Security Breach Management*, if an agent breaches or suspects there may have been a breach of this policy or its procedures.

S12: POLICY AND PROCEDURES RELATED TO CHANGE MANAGEMENT

HHS/CritiCall has developed and implemented this policy and procedures related to change management. This policy and procedures provides details for receiving, reviewing and determining whether to approve or deny a request for a change to the operational environment of HHS/CritiCall in respect of the CCIS. This policy and procedures identifies the process that must be followed and the requirements that must be satisfied in determining whether to approve or deny a request for change.

The CCIS Data Stewardship Committee is responsible for receiving, reviewing and determining whether to approve or deny a request for a change to the operational environment. This includes a discussion of the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

In the event an Authorized User has requested a change request, they shall complete a CCIS Request for Change form and provide the following details:

- Describe the change requested in sufficient detail for a review to be conducted and a course of action determined;
- Describe the rationale for the change including why the change is necessary; and
- Describe the impact of implementing the change on the operational environment.

This security policy and procedures states that requests for changes to the application itself will be reviewed by the CCIS Data Stewardship Committee and, if approved, forwarded to the CCIS Product Manager for further review and analysis. Operational changes or changes required for ongoing system maintenance will be reviewed by the CCIS Operations Committee and if approved, delegated to the CCIS Help Desk for implementation.

This security policy and procedures outlines the manner in which the decision approving or denying a request for a change to the operational environment and the reasons for the decision are documented as well as the method and format in which the decision is communicated to the requestor. The CCIS Product Manager is responsible for reviewing, consulting with others according to the established criteria and for communicating decisions regarding the approval or denial of a CCIS change request to staff required to play a role in the implementation of the change. The CCIS Product Manager is responsible for communicating in writing to the requestor, whether or not their request has been approved or denied.

If the request for a change to the operational environment is not approved, this policy and procedures requires the CCIS Product Manager to document the change to the operational environment requested, the name of the agent requesting the change, the date that the change was requested and the rationale for the determination that the change should not be implemented.

If the request for a change to the operational environment is approved, this policy and procedures states that the CCIS Product Manager is responsible for determining the time-frame for implementation of the change and the priority assigned to the change requested. This policy and procedures also sets out the criteria upon which these determinations are to be made, the process by

which these determinations are to be made and any documentation that must be completed, provided and/or executed in this regard.

This security policy and procedures also sets out the process for implementation of the change to the operational environment, including the agent(s) responsible for implementation and any documentation that must be completed, provided and/or executed by the agent(s) responsible for implementation.

In the circumstance in which changes must be tested, the HHS/CritiCall delegated agent(s) shall test the changes in the test environment prior to implementing changes to the operational environment. This policy and procedures also outlines the documentation that must be completed, provided and/or executed by the agent(s) responsible for testing.

This security policy and procedures also requires documentation to be maintained of changes that have been implemented and identifies the CCIS Product Manager as being responsible for maintaining this documentation. This policy and procedures requires the documentation to include the following particulars:

- A description of the change requested;
- The name of the agent requesting the change;
- The date that the change was requested;
- The priority assigned to the change;
- The date that the change was implemented;
- The agent(s) responsible for implementing the change;
- The date, if any, when the change was tested;
- The agent(s) responsible for testing; and
- Whether or not the testing was successful.

This security policy and procedures requires HHS/CritiCall agents to comply with this policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of a breach. This policy and procedures also stipulates that compliance will be audited in accordance with the *Policy and Procedures In Respect of Security Audits*, on an annual basis by the CritiCall Security Lead. The CritiCall Security Lead is responsible for ensuring compliance with this policy and procedures.

This security policy and procedures also requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the S17 - *Policy and Procedures for Information Security Breach Management*, if an agent breaches or suspects there may have been a breach of this policy or its procedures.

S13: POLICY AND PROCEDURES FOR BACK-UP AND RECOVERY OF RECORDS OF PERSONAL HEALTH INFORMATION

HHS/CritiCall has developed and implemented this security policy and procedures with respect to back-up and recovery (B & R) of records of PHI. The purpose of this policy is to ensure the processes for B & R of PHI in CCIS are conducted according to best practices; ensure that PHI records are

available when needed; ensure testing of related devices; and ensure B & R is conducted properly. Backed-up records must be available for recovery on demand.

This security policy and procedures identifies that HHS/CritiCall has two types of back-up storage devices: (1) Incremental Back-Up (occurs at a minimum on a daily basis); and (2) Full Back-Up (occurs at a minimum on a weekly basis). The CritiCall Security Lead is responsible for the back-up and recovery of records of PHI. This policy and procedures also sets out the process that must be followed and the requirements that must be satisfied in this regard. Backed-up records, which contain PHI, shall be retained in a secure location in compliance with *S5: Policy and Procedures for Secure Retention of Records of Personal Health Information.* This policy and procedures includes particulars regarding documentation that must be completed, provided and/or executed by the agent responsible for testing; identifies the CritiCall Security Lead as being responsible for completing, providing and/or executing the documentation; stipulates the agent(s) to whom this documentation must be provided; and the required content of the documentation.

This security policy and procedures states that the CritiCall Manager, IT is responsible for ensuring that on at least a quarterly basis, a delegate tests the process for the back-up and recovery of records of PHI.

The policy outlines the process to be followed in conducting the back-up and recovery test. The agent completing the test is required to document the date and time of the test; the name of the individual and title of the individual who conducted the test; and the outcome of the test. This comprises the Test Report. The Test Report must be provided to the CritiCall Manager, IT on completion of the test and shall be reviewed by the CritiCall Manager, IT who will notify the CritiCall Security Lead and CCIS Product Manager of any unexpected findings.

The CritiCall Manager, IT, is responsible for ensuring that the back-up and recovery process is completed in accordance with the developed schedule. The Manager, IT may delegate the task of completing the back-up to an appropriate agent.

The agent responsible for back-up and recovery of data shall ensure that back-ups are stored on secure devices and in a secure manner consistent with the requirements set out in *S5: Policy and Procedures for Secure Retention of Records of Personal Health Information* and S6: *Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices*.

The agent shall ensure that back-up devices containing records of PHI reside on-site for a minimum of six (6) months in a secure data centre with appropriate security controls implemented to protect sensitive data from unauthorized access or modification. After such time, records shall be archived and transferred to a secure facility for storage in accordance with *S7: Policy and Procedures for Secure Transfer of Records of Personal Health Information.*

This policy and procedures indicates that the Manager, IT must also maintain documentation in relation to the transfer of backed-up records of PHI to the third party service provider for secure retention. The documentation must address the following particulars, as appropriate:

- That records containing PHI have been transferred to a third party service provider;
- Who was responsible for transferring the records;

- The mode of transfer;
- Who received the records; and
- Confirmation of receipt of transfer of PHI by third party service provider along with confirmation of secure storage of the records.

This policy and procedures permits HHS/CritiCall to contract with a third party service provider to retain backed-up records of PHI. This security policy and procedures requires the backed-up records of PHI to be transferred to and from the third party service provider in a secure manner. This policy and procedures also details the procedure to be followed in securely transferring the backed-up records of PHI to the third party service provider and in securely retrieving the backed-up records of PHI from the third party service provider, including the secure manner in which they will be transferred and retrieved, the conditions pursuant to which they will be transferred and retrieved and the agent(s) responsible for ensuring the secure transfer and retrieval of the backed-up records. In this regard, the procedures shall comply with the S7 - *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.

This security policy and procedures requires all third party service providers contracted to back-up records of PHI on behalf of HHS/CritiCall to enter into a written agreement with HHS/CritiCall that must be executed prior to the third party handling any PHI. The CritiCall Manager IT is responsible for ensuring that a Third Party Agreement is executed and contains the language found within the *P20: Template Agreement for All Third Party Service Providers,* prior to the third party handling any PHI. This includes at a minimum:

- The procedures to be followed in securely transferring the back-up records of PHI to the third party service provider and in securely retrieving the back-up records from the third party service provider and procedures shall comply with the *S7 - Policy and Procedures for Secure Transfer of Records of Personal Health Information;* and
- The manner in which, the date, time and mode of transfer of back-up will be documented which will include a written confirmation from the third party confirming receipt of transfer of PHI.

This security policy and procedures further addresses the need for the availability of backed-up records of PHI, including the circumstances in which the backed-up records are required to be made available.

This security policy and procedures requires all HHS/CritiCall agents to comply with this policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of a breach. This security policy and procedures also stipulates that compliance will be audited in accordance with the S15 - *Policy and Procedures In Respect of Security Audits*, on an annual basis by the CritiCall Security Lead. The CritiCall Security Lead is responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

This security policy and procedures also requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the S17 - *Policy and Procedures for Information Security Breach Management*, if an agent breaches or suspects there may have been a breach of this policy or its procedures.

S14: POLICY AND PROCEDURES ON THE ACCEPTABLE USE OF TECHNOLOGY

HHS/CritiCall has developed and implemented this policy and procedures to outline the acceptable use of CCIS and any related information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by HHS/CritiCall; and sets out the uses that are prohibited; the uses that are permitted; and the uses that are permitted only with prior approval.

For those uses that are permitted only with prior approval, this policy and procedures identifies the CritiCall Security Lead as being responsible for receiving, reviewing and determining whether to approve or deny the request and the process that must be followed and the requirements that must be satisfied in this regard. This policy and procedures outlines the following particulars:

- A discussion of any documentation that must be completed, provided and/or executed;
- The agent(s) responsible for completing, providing and/or executing the documentation;
- The agent(s) to whom this documentation must be provided;
- The required content of the documentation;
- The criteria that must be considered by the CritiCall Security Lead who is responsible for determining whether to approve or deny the request.

This security policy and procedures also identifies the conditions and restrictions with which agents granted approval must comply.

This security policy and procedures identifies the CritiCall Security Lead as the responsible party for reviewing the request and making a recommendation to the CritiCall Executive Director to approve or deny the request. This policy and procedures requires the CritiCall Security Lead to ensure compliance with *P8: Policy and Procedures for Limiting Agent Access to Personal Health Information*. If the request is reasonable and all conditions are met, the CritiCall Security Lead shall make a recommendation to approve the request to the CritiCall Executive Director.

This security policy and procedures provides that the CritiCall Executive Director is responsible for reviewing the recommendation and forwarding the request to the CCIS Data Stewardship Committee for review and approval. This policy and procedures states the CritiCall Executive Director is responsible for determining whether to approve or deny the request. This policy and procedure directs the CritiCall Executive Director to communicate their decision in writing, via email or regular mail to the requestor, including the reason for denial, if the request has been denied.

This security policy and procedures also states that the CritiCall Executive Director is responsible for communicating the decision to the CritiCall Security Lead who shall provide guidance or direction as required to ensure the requestor who has been approved for access to and use of CCIS PHI is provided with any and all HHS/CritiCall policies and procedures that are reasonable in the circumstances to protect PHI.

This security policy and procedures requires all HHS/CritiCall agents to comply with this policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of a breach. This security policy and procedures also stipulates that compliance will be audited in accordance with the S15 - *Policy and Procedures In Respect of Security Audits*, on an annual basis by the CritiCall Security Lead. The CritiCall Security Lead is responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

This security policy and procedures also requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the S17 - *Policy and Procedures for Information Security Breach Management*, if an agent breaches or suspects there may have been a breach of this policy or its procedures.

S15: POLICY AND PROCEDURES IN RESPECT OF SECURITY AUDITS

HHS/CritiCall has developed and implemented this policy and procedures that sets out the types of security audits that are required to be conducted. This policy and procedures requires that a minimum, audits to assess compliance with implemented security policies, procedures and practices; threat risk assessments; security reviews or assessments; vulnerability assessments; penetration testing; ethical hacks and reviews of system control and audit logs be conducted.

With respect to each security audit that is required to be conducted, the policy sets out the purpose of the audits; the nature and scope of the security audit; the agent(s) responsible for conducting the security audit; and the frequency with which and the circumstances in which each security audit is required to be conducted. This policy and procedures requires that a security audit schedule is developed on an annual basis and identifies the CritiCall Security Lead as being responsible for developing the security audit schedule.

The policy and procedures sets out the process to be followed in conducting each audit, including the criteria that must be considered in selecting the subject matter of the audit and whether or not notification will be provided of the audit, and if so, the nature and content of the notification and to whom the notification must be provided. The policy and procedures includes details of the documentation that must be completed, provided and executed in undertaking each security audit; the agent(s) responsible for this; to whom the documentation will be provided; and the required content of the documentation. The CritiCall Security Lead is responsible for ensuring security audits are completed and provided to the CritiCall Executive Director.

The day-to-day management of the privacy program and the security program has been delegated to the CritiCall Privacy Lead and the CritiCall Security Lead respectively.

This policy and procedures sets out the process that must be followed in addressing the recommendations arising from security audits. This policy and procedures states the CritiCall Security Lead shall maintain a log of security audits and shall, in collaboration with the CritiCall Executive Director, monitor the status of the implementation of the recommendations arising from the security audits. This policy and procedures states that it is the responsibility of the CritiCall Executive Director or delegate to assign the individual responsible for addressing the recommendations identified in the audit; ensuring timelines are established to address the

recommendations and for monitoring and ensuring the implementation of the recommendations according to the timelines.

The policy and procedures sets out the nature of the documentation that must be completed, provided and/or executed at the conclusion of the security audit, which includes a written report identifying details of all findings as well as any recommendations. The CritiCall Security Lead is responsible for completing and providing this documentation to the CritiCall Executive Director.

In addition to the written report, the policy and procedures requires that immediately upon completion, audit reports including recommendations arising from the security audits are forwarded by the CritiCall Security Lead to the CritiCall Executive Director. The CritiCall Executive Director is responsible for further communicating the findings of the security audit; the time frame within which the findings of the security audit must be communicated.

The policy and procedures further requires that a log of security audits be maintained by the CritiCall Security Lead. The CritiCall Security Lead is further responsible for tracking that the recommendations arising from the security audits are addressed within the identified time frame and that the CritiCall Executive Director is updated on progress on a monthly basis. Documentation related to security audits will be retained by the Security Lead in a secure location on the CritiCall internal network drive.

This security policy and procedures requires all HHS/CritiCall agents to comply with this policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of a breach. This security policy and procedures also stipulates that compliance will be audited in accordance with the S15 - *Policy and Procedures In Respect of Security Audits*, on an annual basis by the CritiCall Security Lead. The CritiCall Security Lead is responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

This security policy and procedures also requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the S17 - *Policy and Procedures for Information Security Breach Management*, if an agent breaches or suspects there may have been a breach of this policy or its procedures.

S16: LOG OF SECURITY AUDITS

HHS/CritiCall has implemented and maintains a log of security audits that have been completed. The CritiCall Security Lead is responsible for maintaining the Log of Security Audits which includes the following information:

- Nature and type of security audit conducted;
- The date that the security audit was completed;
- The agent(s) responsible for completing the security audit;
- The recommendations arising from the security audit;
- The agent(s) responsible for addressing each recommendation;
- The date that each recommendation was or is expected to be addressed; and
- The manner in which each recommendation was or is expected to be addressed.

S17: POLICY AND PROCEDURES FOR INFORMATION SECURITY BREACH MANAGEMENT

HHS/CritiCall has developed and implemented this policy and procedures to address the identification, reporting, containment, notification, investigation and remediation of information security breaches. This policy and procedures includes a definition of the term "information security breach" which includes any contravention of the security policies, procedures or practices implemented by the HHS/CritiCall as well as an unauthorized person gaining access to, or attempting to gain access to, secured premises or secured information, by any means whatsoever; whenever PHI is or is believed to be stolen, lost; or an act that compromises the confidentiality, integrity (accuracy and completeness), or availability of secured information.

The policy and procedures imposes a mandatory requirement on agents to notify HHS/CritiCall of an information security breach or suspected information security breach.

The policy and procedures identifies the CCIS HelpDesk as the agent who must be notified of the information security breach or suspected information security breach and includes the 24/7 contact information for the CCIS HelpDesk. This policy and procedures stipulates that the CCIS HelpDesk must be notified at the first reasonable opportunity of a breach or suspected information security breach. Notification may be provided verbally and/or in writing and include: the name and contact information of the person reporting the breach/suspected breach; the nature of the incident/circumstances leading the individual to report the breach/suspected breach; when the incident occurred; where the incident occurred; who was involved in the incident; whether PHI was involved in the incident; and any actions taken to contain the situation. The CCIS HelpDesk must complete a CCIS Incident Report Form at the time they are notified of the breach or suspected information security breach, which includes the above information.

The CCIS HelpDesk must immediately notify the CritiCall Executive Director or the Administrator on-call of the actual or suspected information security breach. Notification to the CritiCall Executive Director or Administrator on-call may be provided in writing and/or verbally and must include the information documented on the CCIS Incident Report Form.

This policy and procedures states that upon notification, a determination must be made of whether an information security breach has in fact occurred, and if so, what if any PHI has been breached. This policy and procedures states that the CritiCall Executive Director in collaboration with the CritiCall Manager, IT, must determine the extent of the information security breach and whether the breach is an information security breach or privacy breach or both.

This security policy and procedure addresses the process to be followed where the breach is a privacy breach as well as an information security breach and when the breach is reported as an information security breach but is determined to be a privacy breach. All HHS/CritiCall agents must follow the same policy that governs its management of privacy breaches, namely, *P29: Policy and Procedures for Privacy Breach Management*.

The CCIS HelpDesk must immediately notify the CritiCall Executive Director or the Administrator on-call of the actual or suspected information security breach. Notification to the CritiCall Executive Director or Administrator on-call may be provided in writing and/or verbally and must include the information documented on the CCIS Incident Report Form.

This policy and procedures requires that containment be initiated immediately and CritiCall Executive Director or delegate as being responsible for containment. This policy and procedures outlines the procedure that must be followed in this regard, including any documentation that must be completed, provided and/or executed by the CritiCall Executive Director or delegate and the required content of the documentation. In undertaking containment, this policy and procedures requires that reasonable steps are taken in the circumstances to ensure that additional information security beaches cannot occur through the same means.

This security policy and procedures identifies the CritiCall Executive Director or delegate, as being responsible for reviewing the containment measures implemented and determining whether the information security breach has been effectively contained or whether further containment measures are necessary. This policy and procedures requires the delegate to keep the CritiCall Executive Director apprised of the status of containment measures. The delegate responsible for the containment measures must complete a Containment Report that includes details of the breach, containment measures and review of the success of those measures, and any next steps in the containment process.

This security policy and procedures states that the Containment Report must be provided to the CritiCall Executive Director.

This policy and procedures requires the health information custodian or other organizations that disclosed the PHI to HHS/CritiCall to be notified at the first reasonable opportunity whenever PHI is or is suspected to be stolen, lost or accessed by unauthorized persons and whenever required pursuant to the agreement with the health information custodian or other organization. The HHS Legal Counsel and Chief Privacy Officer, or delegate, is responsible for providing this notification. The notification must be provided in writing and include the extent of the information security breach; the nature of the personal health information at issue, if any; the measures implemented to contain the information security breach; and further actions that will be undertaken with respect to the information security breach, including investigation and remediation.

The policy and procedures sets out whether any other persons or organizations must be notified of the information security breach and sets out the CritiCall Executive Director or delegate as responsible for notifying these other persons or organizations, the format of the notification, the nature of the information that must be provided upon notification and the time frame for notification.

This security policy and procedures stipulates that once containment measures have been completed, the CritiCall Security Lead will initiate an investigation into the information security breach and document the outcome of the investigation, including any recommendations which are documented in the Security Breach Log. This policy and procedures outlines the nature and scope of the investigation (i.e. document reviews, interview, site visits, inspections), the process that must be followed and the documentation that must be completed. Completed documentation must be provided to the CritiCall Executive Director and HHS Chief Information Security Officer, immediately on completion.

Reports of investigations will be retained in a secure section of the HHS/CritiCall document repository. The reports will be maintained by the CritiCall Security Lead.

This security policy and procedures requires the CritiCall Executive Director to assign agents to address the recommendations that have been identified through the investigation process. The

CritiCall Executive Director shall assign activities and timelines associated with the activities to the responsible individuals or business units. If the activities involve those outside of CritiCall, the CritiCall Executive Director shall escalate the requirements to the appropriate party for execution. The CritiCall Security Lead is responsible for monitoring and ensuring that the recommendations are implemented within the stated timelines. This policy and procedures sets out the nature of the documentation that must be completed, provided and/or executed at the conclusion of the investigation of the information security breach. This policy and procedures requires the activities, timelines and responsible individuals to be entered into a Security Breach Log maintained by the CritiCall Security Lead and stored in a secure section of the CritiCall document repository. The nature of the documentation is also outlined in this policy and procedure.

The security policy and procedures also provides that the CritiCall Security Lead is required to provide reports on the progress of recommendations to the CritiCall Executive Director and the CritiCall Enterprise Risk Management Committee according to the set reporting schedule.

This policy and procedure states that all HHS/CritiCall agents must comply with the policy and its procedures and addresses how and by whom compliance will be enforced and the consequences of breach. The policy and procedures also stipulates that compliance will be audited in accordance with the *Policy and Procedures In Respect of Security Audits*, on an annual basis by the CritiCall Security Lead. The CritiCall Security Lead is responsible for conducting the audit and for ensuring compliance with the policy and its procedures.

S18: LOG OF INFORMATION SECURITY BREACHES

HHS/CritiCall has implemented and maintains a log of information security breaches. The CCIS Help Desk is responsible for maintaining the Log of Information Security Breaches. This security policy and procedures requires the following information:

- The date of the information security breach;
- The date that the information security breach was identified or suspected;
- The nature of the PHI, if any, that was the subject matter of the breach and the nature and extent of the breach;
- The date that the information security breach was contained and the nature of containment measures;
- The date that the HIC or other organization that disclosed the PHI to HHS/CritiCall was notified, if applicable;
- The date that the investigation of the breach was completed;
- The agent(s) responsible for conducting the investigation;
- The recommendations arising from the investigation;
- The agent(s) responsible for addressing each recommendation;
- The date each recommendation was or is expected to be addressed; and
- The manner in which each recommendation was or is expected to be addressed.

PART 3 – HUMAN RESOURCES DOCUMENTATION

H1: POLICY AND PROCEDURES FOR PRIVACY TRAINING AND AWARENESS

HHS/CritiCall has developed and implemented a policy and procedures that requires all agents to attend initial privacy orientation as well as ongoing privacy training.

The policy and procedures requires that all staff attend initial privacy training prior to being granted access to any PHI or systems containing PHI. Staff with CCIS-related responsibilities are further required to attend role-based CCIS privacy and security training prior to being granted access to the CCIS and annually thereafter. In addition, all HHS/CritiCall staff are required to attend HHS new staff orientation within six weeks of hire, which includes additional privacy training. All HHS/CritiCall staff are further required annually to complete online privacy training through HHS e-learning system.

The HHS Legal Counsel and Chief Privacy Officer is responsible for preparing and delivering the initial privacy orientation provided during HHS new staff orientation as well as for preparing and making available the annual online privacy training module for all HHS staff.

The CritiCall Privacy Lead is responsible for developing and delivering the initial privacy training for CritiCall staff as well as ongoing privacy training for agents with CCIS role-related responsibilities.

The policy and procedures requires the hiring manager to notify the CritiCall Privacy Lead via e-mail, of the new staff member's start date and role specific access requirements. The CritiCall Privacy Lead shall immediately schedule and the employee shall attend, general privacy training prior to being granted access to CCIS and any PHI or to systems that contain PHI.

Following the general privacy training, the CritiCall Privacy Lead shall schedule, and the employee shall attend, CCIS role-specific privacy training prior to being granted access to CCIS and any PHI or to systems that contain PHI.

The hiring manager shall also schedule and the new employee shall attend new staff orientation which includes additional privacy training provided by the HHS Legal Counsel and Chief Privacy Officer. This shall occur within six weeks of hire. Attendance at this session is logged by HHS. In the event that a new employee fails to attend, the hiring manager shall be notified and the employee will be rescheduled to attend the next session.

The policy and procedures requires that initial privacy training is formalized and standardized and includes the following:

- A description of the status of HHS/CritiCall under the *Act* and the duties and responsibilities that arise as a result of this status;
- A description of the nature of the personal health information collected and from whom this information is typically collected;

- An explanation of the purposes for which personal health information is collected and used and how this collection and use is permitted by the *Act* and its regulation;
- Limitations placed on access to and use of personal health information by agents;
- A description of the procedure that must be followed in the event that an agent is requested to disclose personal health information;
- An overview of the privacy policies, procedures and practices that have been implemented by HHS/CritiCall and the obligations arising from these policies, procedures and practices;
- The consequences of breach of the privacy policies, procedures and practices implemented;
- An explanation of the privacy program, including the key activities of the program and the agent(s) that have been delegated day-to-day authority to manage the privacy program;
- The administrative, technical and physical safeguards implemented by HHS/CritiCall to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal;
- The duties and responsibilities of agents in implementing the administrative, technical and physical safeguards put in place by HHS/CritiCall;
- A discussion of the nature and purpose of the Confidentiality Agreement that agents must execute and the key provisions of the Confidentiality Agreement; and
- An explanation of the *Policy and Procedures for Privacy Breach Management* and the duties and responsibilities imposed on agents in identifying, reporting, containing and participating in the investigation and remediation of privacy breaches.

The policy and procedures requires that ongoing privacy training is formalized and standardized to ensure that agents understand how to apply the privacy policies, procedures and practices in their day-to-day employment, contractual or other responsibilities; to address any new privacy policies, procedures and practices and significant amendments to existing privacy policies, procedures and practices; and to have regard to any recommendations with respect to privacy training made in privacy impact assessments, privacy audits and the investigation of privacy breaches and privacy complaints. Any role specific privacy education needs resulting from changes to systems, legislation, or other factors will be addressed prior to or at the time of the change through customized education for staff in the affected roles.

The policy and procedures requires that attendance at the initial privacy orientation as well as the ongoing privacy training is logged by the CritiCall Privacy Lead and includes the following information:

- Date of each session;
- Type of awareness session (i.e., role-based);
- Instructor's name;
- List of attendees including:

- User information such as name (first and last);
- Department user belongs to;
- Date of training;
- User signature acknowledging their participation; and
- A summary of training session.

This log is maintained by the CritiCall Privacy Lead on a secure CritiCall network drive. Verification of the employee's attendance and completion of the required privacy training session is provided by email to the staff member's hiring manager and the CCIS Product Manager by the CritiCall Privacy Lead.

The Privacy Lead is responsible for tracking attendance at the initial privacy orientation as well as the ongoing privacy training in the related Log. The Log for tracking attendance that is maintained by the CritiCall Privacy Lead, includes the date of the training; type of training and the employee's name. The Log for tracking attendance is maintained by the Privacy Lead and retained on the secure CritiCall network drive. The policy and procedures requires the CritiCall Privacy Lead to notify the hiring manager of any agents who do not attend the initial privacy orientation or the ongoing privacy training. In the event that an employee fails to attend the required privacy training, the CritiCall Privacy Lead and the employee's supervising manager will reschedule the session to occur within five business days.

The employee's access to the CCIS may be suspended until annual training has occurred and the CCIS Confidentiality Agreement has been renewed.

In accordance with the implemented policy, HHS/CritiCall actively fosters a culture of privacy awareness by discussing potential privacy and security risks in the context in which these risks may be occurring with a focus on developing agents' understanding and mitigating of future risks. This includes sharing media stories that focus on privacy issues and responses by other partners in the health care sector with agents; attending Information and Privacy Commission education sessions to increase knowledge and understanding; providing privacy updates during meetings and encouraging agents to ask questions and share comments or concerns; and ensuring privacy information is up to date and available to the public via CritiCall's website.

The policy requires the CritiCall Privacy Lead to ensure role-specific privacy training is provided to all HHS/CritiCall agents who are expected to access, view, enter or work with PHI in the CCIS at the time of initial orientation prior to being granted access to CCIS, as well as annually and whenever any new privacy policies, procedures or practices are introduced.

All agents and hospital-based users participating in CCIS must comply with this policy and procedures. An audit of compliance with this policy and procedures will be conducted in accordance with the *P27: Policy and Procedures In Respect of Privacy Audits*. The CritiCall Privacy Lead will conduct an audit of compliance with this policy and procedures on an annual basis and report the findings to the CritiCall Executive Director and the HHS Chief Privacy Officer. A compliance report will be provided to the HHS VP, Legal Services and General Counsel and the HHS EVP, Clinical Operations and Chief Operating Officer by the HHS Chief Privacy Officer as part of the annual policy review and audit process.

The policy and procedures requires all agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the P29 - *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures. If a breach of this policy is found to have occurred an investigation will be conducted by the CritiCall Privacy Lead. If a breach, a suspected 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 CritiCall Executive Director 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 Procedures for Privacy Breach Management*.

H2: LOG OF ATTENDANCE AT INITIAL PRIVACY ORIENTATION AND ONGOING PRIVACY TRAINING

HHS/CritiCall has implemented and maintains a log of attendance at initial privacy orientation and ongoing privacy training. The CritiCall Privacy Lead is responsible for maintaining this log which includes the following information:

- Name of the agent;
- The date that the agent attended the initial privacy orientation; and
- The dates that the agent attended ongoing privacy training.

H3: POLICY AND PROCEDURES FOR SECURITY TRAINING AND AWARENESS

HHS/CritiCall has developed and implemented a policy and procedures that requires all agents to attend initial security orientation as well as ongoing security training. These sessions are combined with the privacy orientation and ongoing training.

The policy and procedures requires that all staff attend initial privacy and security training prior to being granted access to any PHI or systems containing PHI. Staff with CCIS-related responsibilities are further required to attend role-based CCIS privacy and security training prior to being granted access to the CCIS and annually thereafter.

The CritiCall Privacy Lead, in conjunction with the CritiCall Security Lead, is responsible for developing and delivering the initial privacy and security training for CritiCall staff as well as ongoing privacy and security training for agents with CCIS role-related responsibilities.

The policy and procedures requires that the hiring manager is responsible for notifying the CritiCall Privacy Lead via e-mail, of the new staff member's start date and role specific access requirements. The CritiCall Privacy Lead shall immediately schedule and the employee shall attend, general privacy and security training prior to being granted access to CCIS and any PHI or to systems that contain PHI.

Following the general privacy training, the CritiCall Privacy Lead shall schedule, and the employee shall attend, CCIS role-specific privacy and security training prior to being granted access to the CCIS and any PHI or to systems that contain PHI.

The policy and procedures requires that attendance at the initial privacy and security orientation as well as the ongoing privacy and security training is logged by the CritiCall Privacy Lead and includes the following information:

- An overview of the security policies, procedures and practices that have been implemented by HHS/CritiCall and the obligations arising from these policies, procedures and practices;
- The consequences of breach of the security policies, procedures and practices implemented;
- An explanation of the security program, including the key activities of the program and the agent(s) that have been delegated day-to-day authority to manage the security program;
- The administrative, technical and physical safeguards implemented by HHS/CritiCall to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal;
- The duties and responsibilities of agents in implementing the administrative, technical and physical safeguards put in place by HHS/CritiCall; and
- An explanation of the S17 - *Policy and Procedures for Information Security Breach Management* and the duties and responsibilities imposed on agents in identifying, reporting, containing and participating in the investigation and remediation of information security breaches.

The policy and procedures requires that ongoing privacy and security training is formalized and standardized to ensure that agents understand how to apply the privacy and security policies, procedures and practices in their day-to-day employment, contractual or other responsibilities; to address any new privacy or security policies, procedures and practices and significant amendments to existing privacy and security policies, procedures and practices; and to have regard to any recommendations with respect to privacy and security training made in privacy impact assessments, privacy audits and the investigation of privacy or security breaches and the conduct of security audits including threat and risk assessments, security reviews or assessments, vulnerability assessments, penetration testing, ethical hacks and reviews of system control and audit logs.

The policy and procedures requires that attendance at the initial privacy and security orientation as well as the ongoing privacy and security training is logged by the CritiCall Privacy Lead and includes the following information:

- Date of each session;
- Type of awareness session (i.e., role-based);
- Instructor's name;
- List of attendees including:
- User information such as name (first and last);
- Department user belongs to;

- Date of training;
- And;
- A summary of training session.

This log is maintained by the CritiCall Privacy Lead on a secure CritiCall network drive. Verification of the employee's attendance and completion of the required privacy and security training session is provided by email to the staff member's hiring manager and the CCIS Product Manager by the CritiCall Privacy Lead.

The Privacy Lead is responsible for tracking attendance at the initial security orientation as well as the ongoing security training in the related Log. The log includes the date of the training; type of training and the employee's name. The attendance sheet is maintained by the Privacy Lead and retained on the secure CritiCall network drive. The policy and procedures requires the CritiCall Privacy Lead to notify the hiring manager of any agents who do not attend the initial security orientation or the ongoing security training. In the event that an employee fails to attend the required training, the CritiCall Privacy Lead and the employee's supervising manager will reschedule the session to occur within five business days.

In accordance with the implemented policy, HHS/CritiCall actively fosters a culture of privacy and security awareness by discussing potential privacy and security risks in the context in which these risks may be occurring with a focus on developing agents' understanding and mitigating of future risks. This includes sharing media stories that focus on privacy and security issues and responses by other partners in the health care sector with agents; attending Information and Privacy Commission education sessions to increase knowledge and understanding; providing privacy and security updates during meetings and encouraging agents to ask questions and share comments or concerns.

The policy requires the CritiCall Security Lead to ensure role-specific security training is provided to all HHS/CritiCall agents who are expected to access, view, enter or work with PHI in the CCIS at the time of initial orientation prior to being granted access to CCIS, annually, and whenever any new security policies, procedures or practices are introduced.

All agents must comply with this policy and procedures. An audit of compliance with this policy and procedures will be conducted in accordance with the *S15: Policy and Procedures In Respect of Security Audits*. The CritiCall Security Lead will conduct an audit of compliance with this policy and procedures on an annual basis as part of the annual policy review and audit process and report findings to the CritiCall Executive Director and the HHS Chief Privacy Officer. The HHS Chief Privacy Officer may request that additional random audits be conducted if needed.

The policy and procedures requires all agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the A17 - *Policy and Procedures for Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures. If a breach of this policy is found to have occurred, an investigation will be conducted by the CritiCall Security Lead. If a breach, a suspected 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 CritiCall Executive Director will be notified and require the CritiCall Security Lead to initiate an investigation. Each investigation will follow the steps outlined within *S17: Policy and Procedures for Security Breach Management*.

H4: LOG OF ATTENDANCE AT INITIAL SECURITY ORIENTATION AND ONGOING SECURITY TRAINING

HHS/CritiCall has implemented and maintains a log of attendance at initial privacy and security orientation and ongoing privacy and security training. The CritiCall Privacy Lead is responsible for maintaining this log which includes the following information:

- Name of agent;
- The date that the agent attended the initial privacy and security orientation; and
- The dates that the agent attended ongoing privacy security training.

H5: POLICY AND PROCEDURES FOR THE EXECUTION OF CONFIDENTIALITY AGREEMENTS BY AGENTS

HHS/CritiCall has developed and implemented a policy and procedures requiring agents to execute a Confidentiality Agreement in accordance with the H6 - *Template Confidentiality Agreement with Agents* at the commencement of their employment, contractual or other relationship with HHS/CritiCall and prior to being given access to PHI. This policy and procedures further requires that a Confidentiality Agreement be executed by agents before they are granted access to the CCIS and on an annual basis thereafter following the completion of their role-based CCIS Privacy and Security training.

The CritiCall Privacy Lead is responsible for ensuring that a Confidentiality Agreement is executed with each agent of HHS/CritiCall at the commencement of the employment, contractual or other relationship and thereafter on an annual basis. The CritiCall Privacy Lead is responsible for ensuring that a Confidentiality Agreement is executed at the time of department role-specific privacy and security annual refresher training, which is generally held during the months of November and December.

The policy and procedures requires that the agent's hiring manager or key contact at HHS/CritiCall (in the case of vendors and agents that are not employees of HHS/CritiCall), notify the CritiCall Privacy Lead, by email, of the upcoming commencement of employment or contract term arrangement with new hires or contracted workers that have CCIS-related duties. The CritiCall Privacy Lead will contact the agent, by e-mail or in person, within two (2) weeks of their onboarding to arrange for the required privacy and security related training as per *H1 – Policy and Procedures for Privacy Training and Awareness* and *H3 – Policy and Procedures for Security Training and Awareness*.

Immediately following the completion of the privacy and security training session(s), the Privacy Lead will provide the agent with a copy of the *H6: CCIS Confidentiality Agreement* and review the terms of the agreement with the agent. The agent will review, sign and return the *H6: CCIS Confidentiality Agreement* within two (2) business days of receipt and prior to being granted access to PHI in the CCIS.

The policy and procedures requires that the CritiCall Privacy Lead keep a log of all completed agreements on the secure section of the CritiCall document repository, along with a scanned copy of executed agreements.

This policy and procedures states that if a signed copy of the *H6: CCIS Confidentiality Agreement* is not returned to the CCIS Privacy Lead within two (2) business days, the CCIS Privacy Lead shall make up to three (3) attempts to contact the agent. If a signed copy of the *H6: CCIS Confidentiality Agreement* is not returned to the CCIS Privacy Lead within one (1) week, the agent's direct manager or key HHS/CritiCall contact shall be notified that the agent failed to return the signed *H6: CCIS Confidentiality Agreement* and the agent's direct manager or key HHS/CritiCall contact will follow up directly with the agent.

This policy and procedures indicates that all agents must comply with this policy and procedures. This policy and procedures requires that an audit of compliance with this policy and procedures will be conducted in accordance with the *P27: Policy and Procedures In Respect of Privacy Audits*. The CritiCall Privacy Lead will conduct an audit of compliance with this policy and procedures on an annual basis and report the findings to the CritiCall Executive Director and the HHS Legal Counsel and Chief Privacy Officer. A compliance report will be provided to the HHS VP Legal and General Counsel and the EVP Clinical Operations and Chief Operating Officer by the HHS Legal Counsel and Chief Privacy Officer as part of the annual policy review and audit process.

The policy and procedures requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the P29 - *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures. If a breach, a suspected breach or a privacy risk with regard to disclosure of PHI is identified by an agent of HHS/CritiCall, they must immediately contact the CCIS Help Desk. The CritiCall Executive Director 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 Procedures for Privacy Breach Management*. Where a breach is found to be intentional or the result of continuous negligent work practices, disciplinary action will be taken up to and including termination of employment and/or laying criminal charges, as per *H11: Policy and Procedures for Discipline and Corrective Action.*

H6: TEMPLATE CONFIDENTIALITY AGREEMENT WITH AGENTS

HHS/CritiCall has developed and implemented a Confidentiality Agreement to be executed with all agents in accordance with the *H5- Policy and Procedures for the Execution of Confidentiality Agreements by Agents.* The agreement addresses the matters set out below.

General Provisions

The Confidentiality Agreement describes the status of HHS/CritiCall under the *Act* and the duties and responsibilities arising from this status. It states that individuals executing the agreement are agents of HHS/CritiCall in respect of PHI and outlines the responsibilities associated with this status.

The Confidentiality Agreement requires agents to comply with the provisions of the *Act* and its regulation relating to prescribed persons and with the terms of the Confidentiality Agreement as may be amended from time to time.

The Confidentiality Agreement includes a statement that requires agents to acknowledge that they have read, understood and agree to comply with the privacy and security policies, procedures and practices implemented by HHS/CritiCall and to comply with any privacy and security policies,

procedures and practices as may be implemented or amended from time to time following the execution of the Confidentiality Agreement.

The Confidentiality Agreement includes definitions of '*Personal Health Information', 'Agent', Confidential Information'* and *'Health Information Custodian'* that are consistent with the Act and P29 - its regulation.

Obligations with Respect to Collection, Use and Disclosure of Personal Health Information

The Confidentiality Agreement identifies the purposes for which agents are permitted to collect, use and disclose PHI on behalf of HHS/CritiCall and any limitations, conditions or restrictions imposed therein.

HHS/CritiCall ensures the purposes for which agents are permitted to collect, use or disclose PHI, that each collection, use or disclosure identified in the Confidentiality Agreement is permitted by the *Act* and its regulation. In this regard, the Confidentiality Agreement prohibits agents from collecting and using PHI except as permitted in the Confidentiality Agreement and from disclosing such information except as permitted in the Confidentiality Agreement or as required by law.

The Confidentiality Agreement further prohibits agents from collecting, using or disclosing PHI if other information will serve the purpose and from collecting, using or disclosing more PHI than is reasonably necessary to meet the purpose.

Termination of the Contractual, Employment or Other Relationship

The Confidentiality Agreement requires agents to securely return all property of HHS/CritiCall, including records of PHI and all identification cards, access cards and/or keys, on or before the date of termination of the employment, contractual or other relationship in accordance with the *H10 - Policy and Procedures For Termination or Cessation of the Employment or Contractual Relationship*. The Confidentiality Agreement stipulates on or before the date of termination any property of HHS/CritiCall must be securely returned in compliance with *S7-Policy and Procedure for Secure Transfer of Records of Personal Health Information* to the agent's direct supervisor or HHS/CritiCall key contact. If the destruction of confidential information/PHI has been agreed to with the supervisor, it will be in compliance with *S8 – Policy and Procedure for Secure Disposal of Records of Personal Health Information*.

Notification

The Confidentiality Agreement requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the *P29 - Policy and Procedures for Privacy Breach Management* and/or the *S17 - Policy and Procedures for Information Security Breach Management*, if the agent breaches or believes that there may have been a breach of the Confidentiality Agreement or if the agent breaches or believes that there may have been a breach of the privacy or security policies, procedures and practices implemented by the prescribed person or prescribed entity.

Consequences of Breach and Monitoring Compliance

The Confidentiality Agreement outlines the consequences of a breach of the agreement and addresses that compliance with the Confidentiality Agreement will be reviewed by HHS/CritiCall on a regular

basis and audited in accordance with *P27 - CCIS Policy and Procedure In Respect of Privacy Audits* and *S15 – Policy and Procedure in Respect of Security Audits*.

H7: LOG OF EXECUTED CONFIDENTIALITY AGREEMENTS WITH AGENTS

HHS/CritiCall has implemented and maintains a log of Confidentiality Agreements that have been executed by agents at the commencement of their employment, contractual or other relationship with HHS/CritiCall and on an annual basis. The log is maintained by the CritiCall Privacy Lead and includes the following information:

- Name of the agent;
- The date of commencement of the employment, contractual or other relationship with HHS/CritiCall; and
- The date that the Confidentiality Agreement was executed.

H8: JOB DESCRIPTION FOR THE POSITION(S) DELEGATED DAY-TO-DAY AUTHORITY TO MANAGE THE PRIVACY PROGRAM

HHS/CritiCall has developed and implemented a job description for the position(s) that have been delegated day-to-day authority to manage the privacy program for the CCIS on behalf of HHS/CritiCall which is documented in *H8 – Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program.*

The job description sets out the reporting relationship of the position(s) that have been delegated day-to-day authority to manage the privacy program to the HHS Chief Executive Officer. These positions include the HHS Chief Executive Officer, HHS; VP Legal and General Counsel, HHS EVP Clinical Services and CEO, HHS Legal Counsel and Chief Privacy Officer, CritiCall Executive Director; and the CritiCall Privacy Lead. The responsibilities and obligations of these position(s) in respect of the privacy program are documented and include the following:

- Developing, implementing, reviewing and amending privacy policies, procedures and practices for the CCIS;
- Ensuring compliance with the privacy policies, procedures and practices implemented;
- Ensuring transparency of the privacy policies, procedures and practices implemented;
- Facilitating compliance with *PHIPA* and its Regulation;
- Ensuring agents are aware of *PHIPA* and its Regulation;
- Ensuring agents are aware of *PHIPA* and its Regulation and their duties thereunder;
- Ensuring agents are aware of the privacy policies, procedures and practices implemented by HHS/CritiCall for the CCIS and are appropriately informed of their duties and obligations thereunder;
- Directing, delivering or ensuing the delivery of the initial privacy orientation and the ongoing privacy training and fostering a culture of privacy;
- Conducting, reviewing, and approving privacy impact assessments;

- Receiving, documenting, tracking, investigating, remediating and responding to privacy complaints pursuant to the *P31: Policy and Procedures for Privacy Complaints*;
- Receiving and responding to privacy inquiries pursuant to the *P33: Policy and Procedures for Privacy Inquiries*;
- Receiving, documenting, tracking, investigating and remediating privacy breaches or suspected privacy breaches pursuant to the *P29: Policy and Procedures for Privacy Breach Management*; and
- Conducting privacy audits pursuant to *P27: Policy and Procedures In Respect of Privacy Audits.*

H9: JOB DESCRIPTION FOR THE POSITION(S) DELEGATED DAY-TO-DAY AUTHORITY TO MANAGE THE SECURITY PROGRAM

HHS/CritiCall has developed and implemented a job description for the position(s) that have been delegated day-to-day authority to manage the security program on behalf of HHS/CritiCall which is documented in *H9 – Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program*.

The job description sets out the reporting relationship of the position(s) that have been delegated day-to-day authority to manage the security program to the HHS Chief Executive Officer. These positions include the HHS Chief Executive Officer, HHS VP Legal and General Counsel, HHS EVP Clinical Operations and Chief Operating Officer, HHS CritiCall Executive Director, and the CritiCall Security Lead. The responsibilities and obligations of these position(s) in respect of the security program are documented and include the following:

- Developing, implementing, reviewing and amending security policies, procedures and practices for the CCIS;
- Ensuring compliance with the security policies, procedures and practices implemented;
- Ensuring agents are aware of the security policies, procedures and practices implemented by HHS/CritiCall and are appropriately informed of their duties and obligations thereunder;
- Directing, delivering or ensuring the delivery of the initial security orientation and the ongoing security training and fostering a culture of information security awareness;
- Receiving, documenting, tracking, investigating and remediating information security breaches or suspected information security breaches pursuant to the *S17: Policy and procedures for Information Security Breach Management;* and
- Conducting security audits pursuant to the *S15: Policy and Procedures In respect of Security Audits*.

H10: POLICY AND PROCEDURES FOR TERMINATION OR CESSATION OF THE EMPLOYMENT OR CONTRACTUAL RELATIONSHIP

HHS/CritiCall has developed and implemented *H10 – Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship* which requires agents, as well as their supervisors, to notify HHS/CritiCall of the termination of the employment, contractual or other relationship.

This policy and procedures identifies that notification of the end of employment related to agents who have access to CCIS will be provided to the CritiCall Manager of IT by the agent's direct supervisor or HHS/CritiCall key contact as soon as it becomes known that this is the intent, or, immediately, in the case of termination for cause or other incident resulting in immediate termination of employment or contract. All access to the CCIS and HHS/CritiCall premises shall be de-activated/restricted on termination of employment or contractual relationship.

The policy and procedures includes a definition of "property" as "all physical and virtual assets and information related to the CCIS or that enable HHS/CritiCall employees, contractors, or others to access the CCIS or its information. This includes but is not limited to all records of personal health information (PHI), employee identification cards, access cards and/or keys to physical premises that contain CCIS hardware, software, data, data scripts, records or copies of records or related information" and requires that all property of HHS/CritiCall be securely returned on or before the date of termination.

The policy and procedures identifies that the hiring manager or HHS/CritiCall key contact is responsible for advising the agent that they must surrender, prior to the End of Employment, all PHI and any HHS/CritiCall related assets including: any keys, access cards and ID badges issued to the agent; and all HHS/CritiCall CCIS related assets such as computer, mobile phone, pager, USB keys or paper documents/files that may contain PHI issued to the agent. All property must be securely returned to the hiring manager within one (1) week notice of termination or employment/contract cessation.

The policy and procedures identifies the CritiCall Manager of IT as being responsible for notifying the CCIS Help Desk to: de-activate the agent's network access account(s); de-activate the agent's CCIS access account(s); de-activate the agent's access to the HHS/CritiCall premises; and log the CCIS access termination in *P9: Log of Agents Granted Approval to Access and Use Personal Health Information.* Once all property has been returned, the CritiCall Manager of IT will: check the agents computer(s) for the presence of PHI and either archive any PHI found on the individual's computer(s) according to the *S5: Policy and Procedures for the Secure Retention of Records of Personal Health Information* or destroy any PHI found on the agent's computer(s) according to *S8: Policy and Procedures for Secure Disposal of Records of Personal Health* Information; and check the agent's physical workspace for any portable media or printed information that may contain PHI. The CritiCall Manager of IT or delegate is responsible for completing the Asset Inventory Log for all agents terminating employment with HHS/CritiCall.

The policy and procedures states that in the event that property is not received within the designated time period, the hiring manager or HHS/CritiCall key contact will inform the CritiCall Executive Director. The CritiCall Executive Director is responsible for notifying the CritiCall Privacy Lead, the CritiCall Security Lead and appropriate HHS personnel, and may take action, including:

- Notifying the police of physical property loss;
- Executing the Breach Management Protocol as per *S17: Policy and Procedures for Information Security Breach Management* to address suspected breaches to security or *P29: Policy and Procedures for Privacy Breach Management* for suspected breaches to privacy;
- Notifying the Information Privacy Commissioner of Ontario, as required; and
- Taking legal action to recover property.

HHS/CritiCall requires all agents to comply with this policy and its procedures. In accordance with this policy and procedures, the CritiCall Privacy Lead is responsible for ensuring that all terminations and cessation of employment matters proceed in compliance with the provisions of this document. An audit of compliance will be conducted annually by the HHS Legal Counsel and Chief Privacy Officer in accordance with the audit criteria and reporting requirements outlined within *P27: Policy and Procedures in Respect of Privacy Audits* and *S15: CCIS Policy and Procedures In Respect of Security Audits.* Additionally, supplementary reviews will also be conducted quarterly by the CritiCall Security Lead to ensure the CCIS is not being accessed through accounts assigned to terminated parties.

This policy and procedures requires agents to notify HHS/CritiCall at the first reasonable opportunity, in accordance with the P29- *Policy and Procedures for Privacy Breach Management* and/or S17- *Policy and Procedures for Information Security Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures. An investigation will be conducted by the CritiCall Privacy Lead in accordance with *P29: CCIS Policy and Procedures for Privacy Breach Management*.

H11: POLICY AND PROCEDURES FOR DISCIPLINE AND CORRECTIVE ACTION

HHS/CritiCall has developed and implemented *H11 – Policy and Procedures for Discipline and Corrective Action* in respect of PHI.

This policy and procedures addresses the investigation of disciplinary matters and states that if misconduct or a suspected breach of privacy practices related to the CCIS is identified by the supervising manager of an employee, an investigation will be undertaken. This privacy policy and procedures addresses the procedures that must be followed in undertaking the investigation.

The investigation will be conducted by the CritiCall Privacy Lead and/or CritiCall Security Lead pursuant to *P29: Policy and Procedures for Privacy Breach Management* and/or *S17: Policy and Procedures for Information Security Breach Management*. The CritiCall Privacy Lead or the CritiCall Security Lead will prepare a report outlining the investigation and the evidence of the actions which lead to the breach. A copy of the Privacy Breach Report and/or Security Incident Reports shall be updated by the CritiCall Privacy Lead and/or the CritiCall Security Lead, and provided to the CritiCall Executive Director for recommendations. The CritiCall Executive Director, the employee's supervising manager, and the HHS Chief Privacy Officer will meet to review the details of the investigation and the breach. The severity of the issues will be discussed and reviewed in accordance with the HHS Progressive Discipline Policy which is focused on correcting and clarifying expectations related to behavior(s) that are cause for concern.

This policy and procedures outlines the types of discipline that may be imposed by HHS/CritiCall and the factors that must be considered in determining the appropriate discipline and corrective action. This policy and procedures outlines the agents responsible for determining the appropriate discipline and corrective action, the procedure to be followed in making this determination, the agents that must be consulted in making this determination and the documentation that must be completed, provided and/or executed are also identified.

The following factors will be considered during the discussion:

- The seriousness of the infraction;
- The employee's disciplinary history;
- Length of service;
- Where the infraction took place (private vs. public area); and
- Any unusual conditions or extenuating circumstances.

The team shall make a recommendation of whether the employee should receive a:

- Formal (Recorded) Verbal Warning;
- Formal Written Warning;
- Suspension; or
- Termination.

The CritiCall Executive Director will forward the recommendations to the HHS, Human Resources Business Partner (and the union, if required) for review. The CritiCall Executive Director and the HHS Director, Human Resources shall convene and review the recommendations and determine the appropriate discipline.

The CritiCall Privacy Lead shall update the Privacy Breach Report and *P30: Log of Privacy Breaches* with the final actions taken.

The employee's supervising manager is responsible for retaining any additional documentation in the employee's official Human Resource file.

PART 4 – ORGANIZATIONAL DOCUMENTATION

O1: PRIVACY GOVERNANCE AND ACCOUNTABILITY FRAMEWORK

HHS/CritiCall has developed and implemented a privacy governance and accountability framework for ensuring compliance with the *Act* and its regulation and for ensuring compliance with implemented privacy policies, procedures and practices.

The privacy governance and accountability framework stipulates that the HHS Chief Executive Officer is ultimately accountable for ensuring that HHS/CritiCall and its agents comply with the *Act* and its regulation and implemented privacy policies, procedures and practices.

The HHS CEO has delegated the day-to-day responsibility of oversight for ensuring overall compliance with PHIPA, its regulation to the HHS Chief Privacy Officer. The HHS Chief Privacy Officer , jointly with the CritiCall Executive Director, are delegated to oversee compliance with the Act and its regulation, and for ensuring compliance with the CCIS privacy and security policies, procedures and practices. The CritiCall Executive Director, has appointed a CritiCall Privacy Lead who is responsible for the day-to-day privacy operations, compliance and management.

O1- Privacy Governance and Accountability Framework includes detailed descriptions of each position involved in the day-to-day management of the privacy program including the reporting relationship to the HHS CEO. The policy also includes a schematic of the relationships between these roles.

The framework describes the role of the HHS Board of Directors in respect of the privacy program. The HHS Privacy Office is responsible for preparing a report to the HHS Board of Directors on an annual basis. HHS/CritiCall's framework requires that the Annual Report provided to the HHS Board of Directors must address the initiatives undertaken by the privacy program including privacy training and the development implementation of privacy policies, procedures and practices; the results of any audits or assessments of HHS/CritiCall's privacy and security policies for the CCIS as well as any recommendations made and the status of the implementation of those recommendations. The Board of Directors must also be advised of any privacy breaches and privacy complaints that were investigated including the results of and any recommendations arising from the investigations and the status of those recommendations. The HHS Board Chair may also be notified and briefed of any significant privacy related events by the HHS CEO, at the CEO's discretion.

An organizational chart detailing the relationship of between the HHS Board of Directors, the CritiCall Executive Council, and committees that support the privacy program is included in the framework.

The framework specifies that details of the privacy governance and accountability framework are communicated to all entities and individuals involved in the operational planning and day-to-day activities of the CCIS by either the Chief Privacy Officer ; the CritiCall Privacy Lead; the CCIS Education Team; and/or Participating Hospital designated Privacy Contacts.

The responsible party must provide a hard copy or electronic copy of all documented policies, procedures and practices relevant to the CCIS. Electronic copies are accessible to all CCIS users and other agents with access to the CCIS through the CCIS Document Library.

O2: SECURITY GOVERNANCE AND ACCOUNTABILITY FRAMEWORK

HHS/CritiCall has developed and implemented a security governance and accountability framework for ensuring compliance with the *Act* and its regulation and for ensuring compliance with implemented security policies, procedures and practices.

The security governance and accountability framework stipulates that the HHS Chief Executive Officer is ultimately accountable for ensuring the security of PHI in the CCIS and that HHS/CritiCall and its agents comply with the security policies, procedures and practices implemented.

The HHS CEO has delegated the day-to-day responsibility for the HHS/CritiCall security program for the CCIS to the HHS Chief Information Officer. The CritiCall, Executive Director is responsible for CritiCall and has delegated the responsibility for security to the CritiCall Security Lead. The CritiCall Security Lead reports to the CritiCall Executive Director.

The framework includes detailed descriptions of each position involved in the day-to-day management of the security program including the reporting relationship to the HHS CEO. A schematic of the relationships is included.

The HHS Board of Directors is responsible for oversight of security at HHS. The HHS CIO is responsible for preparing a report to the HHS Board of Directors on an annual basis. HHS/CritiCall's policy and procedures requires that the Annual Report provided to the Board of Directors must address the initiatives undertaken by the security program for the CCIS including security training and the development and implementation of security policies, procedures and practices; the results of any audits or assessments of HHS/CritiCall's privacy and security policies for the CCIS, as well as any recommendations made and the status of the implementation of those recommendations. The HHS Board of Directors must also be advised of any information security breaches for the CCIS that were investigated including the results of and any recommendations arising from the investigations and the status of those recommendations.

An organizational chart detailing the relationship of between the HHS Board of Directors, the CritiCall Executive Council and committees that support the security program is included in the framework.

The Security Governance Accountabilities and Framework for the CCIS is communicated to all entities and individuals involved in the operational planning and day-to-day activities of the CCIS by either the CritiCall Security Lead or Participating Hospital Privacy Contact. The responsible party must provide a hard copy or electronic copy of all documented policies, procedures and practices relevant to the CCIS. Electronic copies are accessible to all CCIS users and other agents with access to the CCIS through the CCIS Document Library.

O3: TERMS OF REFERENCE FOR COMMITTEES WITH ROLES WITH RESPECT TO THE PRIVACY PROGRAM AND/OR SECURITY PROGRAM

HHS/CritiCall has developed and implemented terms of reference for each committee that has a role in respect of the privacy and security programs for the CCIS. The following committees have a role in the privacy and security programs: CritiCall Executive Council; CCIS Data Stewardship Committee; CCIS Operations Committee; and CritiCall Enterprise Risk Management Committee.

HHS/CritiCall's *03 – Terms of Reference for Committees with Roles with Respect to the Privacy Program and/or Security Program* for the CCIS requires that the following details are included for each committee: the membership of the committee, the chair of the committee, the mandate and responsibilities of the committee in respect of the privacy and or the security program for the CCIS; the frequency with which the committee meets; to whom the committee reports; the types of reports produced by the committee; the format of the reports, to whom these reports are presented; and the frequency of these reports.

O4: CORPORATE RISK MANAGEMENT FRAMEWORK

HHS/CritiCall has developed and implemented a comprehensive and integrated corporate risk management framework for the CCIS to identify, assess, mitigate and monitor risks relating to the CCIS, including risks that may negatively affect its ability to protect the privacy of individuals whose PHI is collected through the CCIS and to maintain the confidentiality of that information.

The CritiCall integrated risk management framework for the CCIS identifies the agent(s) responsible and the process that must be followed in identifying risks that may negatively affect the ability of HHS/CritiCall to protect the privacy of individuals whose PHI is collected through the CCIS and to maintain the confidentiality of that information and includes a discussion of the agents or other persons or organizations that must be consulted in identifying the risks; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.

The CritiCall integrated risk management framework for the CCIS sets out the agent(s) responsible, the process that must be followed and the criteria that must be considered in ranking the risks and assessing the likelihood of the risks occurring for the CCIS and the potential impact if they occur. This includes a discussion of the agent(s) or other persons or organizations that must be consulted in assessing and ranking the risks; the documentation that must be completed, provided and/or executed in assessing and ranking the risks; the documentation that must be completed, provided and/or executed in setting out the rationale for the assessment and ranking of the risks; the agent(s) responsible for completing, providing and /or executing the

documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation. The CritiCall integrated risk management framework identifies the agent(s) responsible, the process that must be followed and the criteria that must be considered in identifying strategies to mitigate the actual or potential risks to privacy that were identified and assessed in the CCIS, the process for implementing the mitigation strategies and the agents or other persons or organizations that must be consulted in identifying and implementing the mitigation strategies.

Agent(s) responsible for assigning other agent(s) to implement the mitigation strategies, for establishing timelines to implement the mitigation strategies, and for monitoring and ensuring that the mitigation strategies have been implemented for the CCIS are also included. The CritiCall Executive Director is responsible for assigning agents to implement the mitigation strategies, for establishing timelines to implement those strategies and for monitoring and ensuring that the mitigation strategies have been implemented. The documentation that must be completed, provided and/or executed in identifying, implementing, monitoring and ensuring the implementation of the mitigation strategies; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation is also included.

The manner and format in which the results of the integrated risk management process for the CCIS, including the identification and assessment of risks, the strategies to mitigate actual or potential risks to privacy for the CCIS and the status of implementation of the mitigation strategies, are communicated and reported are included. Agent(s) responsible for communicating and reporting the results of the integrated risk management process for the CCIS, the nature and format of the communication; and to whom the results will be communicated and reported, including to the HHS Chief Executive Officer or the CritiCall Executive Director, are included. Approval and endorsement of the results of the risk management process, including the agent(s) responsible for approval and endorsement, are also included.

The integrated risk management framework for the CCIS requires that a corporate risk register for the CCIS be maintained and reviewed on an ongoing basis in order to ensure that all the risks that may negatively affect the ability of HHS/CritiCall to protect the privacy of individuals whose PHI is received and to maintain the confidentiality of that information in the CCIS continue to be identified, assessed and mitigated. The framework outlines the frequency with which the CCIS risk register must be reviewed and the agent(s) responsible and the process that must be followed in reviewing and amending the CCIS risk register and sets out that the CCIS risk register will be reviewed on a quarterly basis by the CritiCall Executive Council. Amendments to the CCIS Risk Register require prior approval of the CritiCall Executive Director.

The manner in which the CCIS risk management framework will be integrated into the policies, procedures and practices of HHS/CritiCall for the CCIS and into the projects undertaken by HHS/CritiCall for the CCIS and the agent(s) responsible for integration is also addressed and all

risks identified through the CCIS privacy and security policies and procedures and other means including audits, privacy impact assessments and breach incidents must use this framework.

O5: CORPORATE RISK REGISTER

HHS/CritiCall has developed and maintains a CCIS Risk Register. The CCIS Risk Register identifies each risk that may negatively affect the ability of HHS/CritiCall to protect the privacy of individuals whose PHI is received through the CCIS and to maintain the confidentiality of that information.

For each risk identified, the CCIS Risk Register includes the following information: an assessment of the risk; ranking of the risk; the mitigation strategy to reduce the likelihood of the risk occurring and/or to reduce the impact of the risk if it does occur; and the date that the mitigation strategy was implemented or is required to be completed and the responsible agent. The CCIS Risk Register is maintained by the CritiCall Privacy Lead.

O6: POLICY AND PROCEDURES FOR MAINTAINING A CONSOLIDATED LOG OF RECOMMENDATIONS

HHS/CritiCall has developed and implemented a policy and associated procedures requiring a consolidated and centralized log be maintained of all recommendations arising from privacy impact assessments, privacy audits, security audits and the investigation of privacy breaches, privacy complaints and security breaches for the CCIS. The Log is also required to include the recommendations made by the IPC that must be addressed by HHS/CritiCall prior to the next review of its policies, practices and procedures for the CCIS.

The CritiCall Executive Director is responsible for ensuring the Consolidated Log of Recommendations is maintained and updated each time a privacy impact assessment, threat risk assessment, privacy audit, security audit, investigation of a privacy breach, investigation of a privacy complaint, investigation of an information security breach or review by the Information and Privacy Commissioner of Ontario is completed; each time that a recommendation has been addressed; and each time that a review by the CritiCall Executive Council has been conducted.

HHS/CritiCall's policy and procedures requires that the consolidated and centralized log must be reviewed on a quarterly basis, or more frequently, if indicated. The policy and procedures states that on a quarterly basis or more frequently if indicated, the Chair of the CritiCall Executive Council shall add 'Review of Consolidated Log of Recommendations' to the meeting agenda and the Log shall be reviewed by the council members.

The Chair of the CritiCall Executive Council is responsible for adding 'Review of Consolidated Log of Recommendations' to the meeting agenda.

HHS/CritiCall requires all agents to comply with this policy and its procedures. Compliance will be enforced by the HHS Executive Vice President Clinical Operations and Chief Operating Officer. An audit of compliance will be conducted by the HHS CIO on an annual basis and reported to the HHS Executive Vice President Clinical Operations and Chief Operating Officer. The audit criteria and reporting requirements are further outlined within the *P27: Policy and Procedures in Respect of Privacy Audits* and *S15: Policy and Procedures In Respect of Security Audits.*

This policy and procedures requires agents to notify HHS/CritiCall at the first reasonable opportunity in accordance with *P29 - Policy and Procedures for Privacy Breach Management* and *S17 - Policy and Procedures for Security Breach Management*, if any agent breaches or believes there many have been a breach to this policy or its procedures. If a breach, or a suspected breach is identified by any agent, they must immediately contact the CCIS Help Desk. The CritiCall Executive Director will be notified and require the CritiCall Privacy Lead to initiate a privacy investigation or the CritiCall Security Lead to initiate a security investigation. Each investigation will follow the steps outlined within *P29 - Policy and Procedures for Privacy Breach Management* and *S17- Policy and Procedures for Security Breach Management*.

O7: CONSOLIDATED LOG OF RECOMMENDATIONS

HHS/CritiCall has developed and maintains a consolidated log of recommendations arising from privacy impact assessments, privacy and security audits, the investigation of privacy breaches, the investigation of privacy complaints, the investigation of information security breaches, and reviews by the IPC for the CCIS. The information included in the log is as follows:

- Name and date of the document, investigation, audit and/or review from which the recommendation arose;
- Recommendation made;
- The date of the recommendation was addressed or by which it is required to be addressed;
- The manner in which the recommendation was addressed; and
- The agent responsible for addressing the recommendation.

The CritiCall Executive Director is responsible for reviewing reach recommendation to ensure that they are addressed.

O8: BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

HHS/CritiCall has developed and implemented *O8- Business Continuity and Disaster Recovery Plan*, a policy and associated procedures to protect and ensure the continued availability of the information technology environment of HHS/CritiCall for the CCIS in the event of short or long-term business interruptions and in the event of threats to the operating capabilities of the CCIS, including natural, human, environmental and technical interruptions and threats.
The business continuity and disaster recovery plan addresses notification of the interruption or threat, documentation of the interruption or threat, assessment of the severity of the interruption or threat, activation of the business continuity and disaster recovery plan and the recovery of PHI in the CCIS.

In relation to notification of the interruption or threat, the business continuity and disaster recovery plan identifies the agent(s) as well as the other persons or organizations that must be notified of short and long-term business interruptions and threats to the operating capabilities of HHS/CritiCall for the CCIS and the agent(s) responsible for providing such notification and the time frame within which notification must be provided, the manner and format of notification, the nature of the information that must be provided upon notification and any documentation that must be completed, provided and/or executed.

HHS/CritiCall's business continuity and disaster recovery plan for the CCIS identifies that the CritiCall Executive Director or delegate must develop and maintain a contact list of all agents, third party service providers, stakeholders and other persons or organizations that must be notified of business interruptions and threats.

In relation to the assessment of the severity level of the interruption or threat, the business continuity and disaster recovery plan identifies that the CritiCall Executive Director is responsible for the assessment, the criteria pursuant to which this assessment is to be made and the agents and other persons or organizations that must be consulted in assessing the severity level of the interruption or threat. This policy and procedures also addresses the documentation that must be completed, provided and/or executed resulting from or arising out of this assessment; the required content of the documentation; the agent(s) to whom the documentation must be provided; and to whom the results of this assessment must be reported.

In relation to the assessment of the interruption or threat, the business continuity and disaster recovery plan for the CCIS sets out the agent(s) responsible and the process that must be followed in conducting an initial impact assessment of the interruption or threat, including its impact on the technical and physical infrastructure and business processes of HHS/CritiCall for the CCIS. This includes the agents and other persons or organizations that are required to be consulted in undertaking the assessment; the requirements that must be satisfied and the criteria that must be utilized in conducting the assessment; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation;

the agent(s) to whom the documentation must be provided; and the agent(s) to whom the results of the initial impact assessment must be communicated.

The business continuity and disaster recovery plan for the CCIS identifies the agent(s) responsible for conducting and preparing a detailed damage assessment in order to evaluate the extent of the damage caused by the threat or interruption and the expected effort required to resume, recover and restore infrastructure elements, information systems and/or services. The plan addresses the manner in which the assessment is required to be conducted; the agents and other persons or organizations that are required to be consulted in undertaking the assessment; the requirements that must be satisfied and the criteria that must be considered in undertaking the assessment; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the agent(s) to whom the results of the assessment must be communicated.

The business continuity and disaster recovery plan identifies the agent(s) responsible for resumption and recovery, the procedure that must be utilized in resumption and recovery for each critical application and business function, the prioritization of resumption and recovery activities, the criteria pursuant to which the prioritization of resumption and recovery activities is determined, and the recovery time objectives for critical applications. The business continuity and disaster recovery plan includes a discussion of the agents and other persons or organizations that are required to be consulted with respect to resumption and recovery activities; the documentation that must be completed, provided and/or executed; the required content of the documentation; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the agent(s) to whom the results of these activities must be communicated.

The business continuity and disaster recovery plan requires that an inventory be developed and maintained of all critical applications and business functions and of all hardware and software, software licences, recovery media, equipment, system network diagrams, hardware configurations, software configuration settings, configuration settings for database systems and network settings for firewalls, routers, domain name servers, email servers and the like for the CCIS. The business continuity and disaster recovery plan for the CCIS identifies the agent(s) responsible for developing and maintaining the inventory, the agent(s) and other persons and organizations that must be consulted in developing the inventory, and the criteria upon which the determination of critical applications and business functions is made.

The business continuity and disaster recovery plan includes the procedure by which decisions are made and actions taken during business interruptions and threats to the operating capabilities of HHS/CritiCall for the CCIS will be documented and communicated and by whom they will be communicated.

The business continuity and disaster recovery plan for the CCIS also addresses how the testing, maintenance and assessment of the business continuity and disaster recovery plan will occur. In accordance with the plan, the CritiCall Executive Director shall appoint a delegate to plan and

execute testing on an annual basis. The business continuity and disaster recovery plan for the CCIS further identifies the agent(s) responsible for maintaining and assessing the plan; the agent(s) responsible for amending the plan as a result of testing; the procedure to be followed in testing, maintaining, assessing and amending the plan; and the agent(s) responsible for approving the business continuity and disaster recovery plan and any amendments.

The business continuity and disaster recovery plan for the CCIS further addresses the agent(s) responsible and the procedures to be followed in communicating the plan to all agents, to whom the plan will be communicated, including any amendments, and the method and nature of the communication. The agent(s) responsible for managing communications in relation to the threat or interruption are also identified as are the method and nature of the communication.

PART 5 – PRIVACY AND SECURITY INDICATORS

PRIVACY INDICATORS	
General Privacy Policies, Procedures and Practices	
The dates privacy policies and procedures were reviewed since prior review by the IPC/)	Since the time of last approval by the IPC in 2017, HHS/CritiCall's privacy policies and procedures have been reviewed in accordance with the annual policy review as follows: • • October 2017 • May 2018 • September 2019
Whether amendments were made to existing policies and procedures as a result of the review. If so, a list of the amended privacy policies and procedures. A brief description of the amendments made.	No amendments were made to existing policies during the review conducted in October 2017 and May 2018. The following amendments were made to existing policies during the review conducted in September 2019: • Edits were made to all policies to account for role changes within CritiCall Ontario for a dedicated Privacy Lead position and to HHS's organizational structure with respect to privacy operations. • **P5- List of Data Holdings and P7- Statements of Purpose for Data Holdings Containing Personal Health Information** data element list was updated to include the addition of the neonatal intensive care unit (NICU) data, consistent with the expanded mandate in 2017 by the Ministry to CCSO to include NICU data.
Whether new privacy policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and	No new privacy policies and procedures were developed and implemented as a result of the reviews of privacy policies and procedures for the CCIS undertaken in October 2017, May 2018 and September 2019.

procedures developed and implemented.	
The date that each amended and newly developed privacy policy and procedure was communicated to agents and, the nature of the communication for each policy/procedure.	No new policies were developed as a result of the 2017-2019 reviews. Amendments to Policies, noted above, following the 2019 review were not substantive in nature, so broad communication of the change was not specifically undertaken. No new privacy policies and procedures were developed and implemented as a result of the review of the CCIS privacy policies and procedures undertaken in September 2019.
Whether the communication materials available to the public and other stakeholders were amended as result of the review, and if so, a brief description of the amendments.	The updated P5- List of Data Holdings and P7- Statements of Purpose for Data Holdings Containing Personal Health Information data element list to include the addition of the neonatal intensive care unit (NICU) data, consistent with the expanded mandate in 2017 by the MOHLTC to CCSO to include NICU data was posted on the CritiCall website available to the public and other stakeholders.
Collection	
The number and data holdings containing PHI maintained by the prescribed person.	In its capacity as a prescribed person under PHIPA, HHS/CritiCall maintains one data holding, the CCIS Data Holding.
The number of statements of purpose developed for data holdings containing PHI.	The CCIS Data Holding has one statement of purpose which is contained within P7: Statements of Purpose for Data Holdings Containing Personal Health Information
The number and a list of statements of purpose for data holdings containing PHI that were reviewed since the prior review by the IPC.	The Statement of Purpose for the CCIS Data Holding has been reviewed three times since the prior review by the Information and Privacy Commissioner of Ontario (annually).

Whether amendments were made to existing statements of purpose for data holdings containing PHI as a result of the review, and if so, a list of the amended statements of purpose and, for each statement of purpose amended, a brief description of the amendments made.	HHS/CritiCall Ontario has made amendments to the Statement of Purpose for the CCIS in 2018, following the MOHLTC expanded mandate to CCSO to include NICU data that was implemented during 2018 through 2019 at participating hospitals with NICUs.
Use	
The number of agents granted approval to access and use PHI for purposes other than research.	As of October 31, 2019, there are 22 agents of the prescribed person, HHS/CritiCall (HHS/CritiCall staff and third party service provider staff) approved to access and use PHI for purposes other than research. (In addition, as of October 31, 2019, there are 4,760 agents of participating Ontario hospitals approved to access and use PHI for purposes other than research.)
The number of requests received for the use of PHI for research since the prior review by the IPC.	HHS/CritiCall Ontario has received no requests for the use of PHI for research since the prior review by the IPC.
The number of requests for the use of PHI for research purposes that were granted and that were denied since prior review by the IPC.	No requests for the use of PHI for research have been granted or denied by HHS/CritiCall since the prior review by the IPC.
Disclosure	
The number of requests received for the disclosure of PHI for purposes other than research since prior review by the IPC.	There have been zero requests for the disclosure of PHI for purposes other than research since prior review by the IPC.
The number of requests for the disclosure of PHI for purposes other than research that were granted and that were denied since prior review by the IPC.	No requests for the disclosure of PHI for purposes other than research have been received, granted or denied.
The number of requests received for the disclosure of PHI for research	One request has been received for the disclosure of PHI for research purposes since prior review by the IPC.

purposes since prior review by the IPC.	
The number of requests received for the disclosure of PHI for research purposes that were granted and that were denied since prior review by the IPC.	HHS/CritiCall Ontario has received one request for the disclosure of CCIS PHI data for research purposes research since prior review by the IPC. One request for the disclosure of PHI for research has been granted.
The number of Research Agreements executed with researchers to whom PHI was disclosed since the prior review by the IPC.	One research agreement has been executed with a researcher to whom PHI was disclosed since prior review by the IPC.
The number of requests received for the disclosure of de-identified and /or aggregate information for both research and other purposes since prior review by the IPC.	Zero requests for de-identified/aggregate data for research and other purposes were received since prior review by the IPC.
The number of acknowledgements or agreements executed by persons to whom de-identified and/or aggregate information was disclosed for both research and other purposes since the prior review by the IPC.	Zero Research Agreements or acknowledgements have been executed in relation to the request for de-identified/aggregate data for research and other purposes.
Data Sharing Agreements	
The number of DSAs executed for the collection of PHI by the prescribed person since the prior review by the IPC.	Since the prior review by the IPC, 1 ONE Data Sharing Agreement has been executed with new participating hospital contributing data to the CCIS.
The number of DSAs executed for the disclosure of PHI since prior review by the IPC.	No DSAs have been executed for the disclosure of PHI since prior review by the IPC.

Agreements with Third Party Service Providers	
The number of agreements executed with third party service providers with access to PHI since prior review by the IPC.	No new agreements have been executed with third party service providers since prior review by the IPC. Contract renewal negotiations in 2017, included an update for the inclusion of a Privacy and Security Schedule as recommended by HHS Legal.
Data Linkage	
The number and a list of data linkages approved since the prior review by the IPC.	Zero data linkages were approved since prior review by the IPC.
Privacy Impact Assessments	
The number and a list or PIAs completed since the prior review by the IPC and for each PIA: - The data holding, information system, technology or program - The date of completion of the PIA - A brief description of each recommendation - The date each recommendation was addressed or is proposed to be addressed and - The manner in which each recommendation was addressed or is proposed to be addressed	PIAs COMPLETED SINCE LAST REVIEW: One privacy impact assessment was undertaken in November 2017 and executed by GRA Consultants Inc. The PIA was developed to meet the following objectives: • To identify privacy risks and to recommend strategies to manage those risks. • To demonstrate to stakeholders that HHS/CritiCall has conducted the proper due diligence concerning privacy on the CCIS. The scope of the CCIS PIA analysis included the following: • Personal health information that is processed, stored and transmitted to the CCIS Registry. • Policies, procedures, governance and other administrative components supporting HHS/CritiCall in its role as a prescribed person with respect to the CCIS. The following recommendations were made: • Implement a comprehensive access monitoring and audit program (resolved, January 2019)

	• Conduct a privacy and security breach management exercise and ensure this aligns with the IPC mandatory breach notification requirement (resolved March 2019). • Implement TRA recommendations (resolved, September 2019). An access monitoring and audit program was implemented under the leadership of the CritiCall IT Manager with support from the System Support Specialist team in January 2019. Privacy and Security Breach Management training exercise was conducted with the CritiCall Executive Counsel in March 2019. All TRA recommendations have been implemented as of September 30, 2019. OUTSTANDING ISSUES FROM PAST PIAs: For context, participating hospital systems contribute to the CCIS via their Admissions, Discharge and Transfer (ADT) system. There is a push of ADT data for all participating hospital patients into the CCIS based on an agreed upon schedule. The PHI received from the hospital ADT is received into the CCIS integration database. The data is then moved to a CCIS operations database if it meets 3 specified criteria: 1. It is level 2 or 3 ICU data; 2. It is a recent record; and 3. It is for a patient admitted to the sending hospital. A PIA undertaken in January 2013 by Healthtech Consultants and executed in April 2013 identified that ADT data for patients which do not meet the above noted criteria for transfer into the Operations Database remained in the CCS Integration database for 1 year before being purged.

	The PIA also identified its belief that HHS/CritiCall was making an over collection of data by the receipt of *all* ADT PHI into the CCIS Integration database, instead of only collecting data for those who met the 3 specified criteria. The PIA recommended that CritiCall should review the current ADT push procedure and determine an alternative method which would restrict data collection to only data relating to those patients which met the prescribed 3 criteria. And, that CritiCall should take the necessary steps to ensure that all data that is not transitioned to the operations database is purged in a timely manner. In reviewing the recommendations from the 2013 PIA in an effort to resolve them in 2018, CCIS Manager IT Applications and Security Lead identified that in addition to the above over collection/retention recommendations, some participating hospitals were sending PHI fields in their ADT messages that were not required for the CCIS. Thus, in 2018, it was identified that there were three issues to be resolved: 1. As identified in the 2013 PIA, the perceived over collection of ADT data for all hospital patients, into the integration database (vs. the recommendation that only the data for patients meeting the operations database criteria be collected); 2. The 1-year retention period of data in the Integration Database (vs. the recommendation that that be reduced); and, 3. As identified in 2018 by the CCIS Manager IT, Applications and Security Lead, the over collection of specific data-fields that were not required for either the Integration Database or the Operations Database (vs. the recommendation that these additional data fields be scrubbed and/or a technological solution preventing their collection be implemented).

	In respect of these 3 outstanding issues, HHS/CritiCall has taken the following steps: 1. The perceived over-collection issue identified in the 2013 PIA was reviewed in 2018 and it was determined that it was necessary to collect ADT data for all patients admitted to participating hospitals into the Integration Database, in order to facilitate their transition into the Operations Database should their condition deteriorate in hospital such that they met the specified criteria for inclusion. Absent the collection of their data into the integration database their data would not be available to operationalize as needed within the CCIS. As such, this process was not changed, as it was determined to be necessary for the proper functioning and the stated purposes of the CCIS. This issue is deemed to be resolved. 2. The 1-year retention period in the Integration database was reviewed, and reduced in early 2019 from 1-year to 2 weeks from the date of the relevant patient's discharge for those patients who are never transferred into the Operations Database. The data that is transferred into the Operations Database is retained for 90 days post-discharge for troubleshooting purposes as it is required to resolve system issues that arise, and in order to support participating hospitals in this respect. This issue is deemed to be resolved. 3. Regarding the third issue; that of over-collection of unnecessary/unwanted data fields which was first identified in 2018: a. Our CCIS Product Manager has advised that they have been working to educate participating hospitals on the front-end, to avoid transferring unnecessary data fields thought their ADT, and supporting their efforts to implement appropriate filters (on the hospital side of the transaction) to mitigate against this risk; and,

	b. Working with our third-party vendor to explore potential technological solutions that would prevent hospitals from transmitting data fields outside of those which are required for the purpose of the CCIS. This issue not yet fully resolved, but the risk has been largely mitigated through ongoing efforts and HHS/CritiCall is working towards the ability to implement further solutions as they become available.
The number and a list of PIAs undertaken but not completed since the prior review by the IPC.	No PIAs have been undertaken but not completed since prior review by the IPC.
The number and a list of PIAs that were not undertaken but for which PIAs will be completed and the proposed date of completion.	None.
The number of determinations made since the prior review by the IPC that a PIA is not required and, for each determination, the data holding, information system, technology or program at issue and a brief description of the reasons for the determination.	No determinations were made since the prior review by the IPC that a PIA was not required.
The number and a list of PIAs reviewed since the prior review by the IPC and a brief description of the amendments made.	As noted in Indicator 1, of this section, HHS/CritiCall has resolved all recommendations identified through past PIAs. There remains one outstanding risk item which was identified in 2018 (over-collection of unnecessary data-fields) through processes other than a PIA, for which mitigation/resolution is in progress.

Privacy Audit Program	
The dates of audits of agents granted approval to access and use PHI since the prior review by the IPC and for each audit conducted: - A brief description of the recommendation made - The date each recommendation was addressed or is proposed to be addressed and - The manner in which each recommendations was addressed or is proposed to be addressed	**Refer to Appendix 1 - Privacy Audits for details**
The number and a list of all other privacy audits completed since the prior review by the IPC and for each audit: - A description of the nature and type of audit conducted - The data of completion of the audit - A brief description of the each recommendation made - The date each recommendation was addressed or is proposed to be addressed and - The manner in which each recommendation was addressed or is proposed to be addressed.	**Refer to Appendix 1 - Privacy Audits for details**
Privacy Breaches	
The number of notifications of privacy breaches or suspected privacy breaches received by the prescribed person since the prior review by the IPC.	There have been two notifications of privacy breaches or suspected privacy breaches since prior review by the IPC.

With respect to each privacy breach or suspected privacy breach: - The date that the notification was received - The extent of the privacy breach or suspected privacy breach - Whether it was internal or external - The nature and extent of PHI at issue - The date that senior management was notified - The containment measures implemented - The date(s) that the containment measures were implemented - The date(s) that notification was provided to the HIC or any other organizations - The date the investigation was commenced - The date the investigation was completed - A brief description of each recommendation made - The date each recommendation was addressed or is proposed to be addressed and - The manner in which each recommendation was addressed or is proposed to be addressed	Incident 1 • Notification received from participating hospital authorized User February 5, 2019 to CCIS Help Desk regarding accessing CCIS through another authorized User's CCIS account. • Investigation commenced immediately on February 5, 2019 by CritiCall Privacy Lead. • Containment was immediately undertaken by the CCIS Help Desk by disabling the authorized User account being used to access the CCIS by another authorized User. • Breach was determined to be low risk. CritiCall Privacy Lead spoke with the User and provided retraining on the requirements for protecting privacy in the CCIS including keeping passwords secure and confidential. CCIS Terms of Use reviewed with User. • User advised that Hospital LRA and Privacy Contact had been informed of the incident. • CritiCall Privacy Lead followed up with Privacy Contact at participating hospital who advised that privacy and security awareness retaining would be undertaken with the User. • User was required to complete on-line CCIS privacy training module prior to being permitted to access and use the CCIS through her own account. Prior to accessing and using the CCIS, User was required to agree to and electronically accept the CCIS Terms of Use. • Breach report was submitted to CritiCall Executive Director and the investigation was completed on February 5, 2019. • No further recommendations were made, as the offending user was acting within their role, however doing so inappropriately by using the credentials of another authorized user. Incident 2 • Notification received from the CCIS Help Desk August 12, 2019 that CCIS deployment on August 10, 2019 potentially created an issue for

	Hospital data. Third party service provider (vendor) requested two patient names and MRN numbers from CCIS Help Desk to trouble shoot an identified issue in the CCIS. • CCIS Help Desk staff member emailed through regular email, the MRN numbers of patients names for two patients. • CCIS Help Desk staff member immediately took containment measures by notifying the third party service provider (vendor) to delete the email from their received and deleted email message. The CCIS Help desk staff member immediately deleted the email from the CCIS Help Desk ticket and from deleted folder. • CritiCall Privacy lead provided reminder email communication to all Users at CritiCall with access to PHI in the CCIS about not emailing identifiable PHI. • The investigation commenced on August 12, 2019 as it was determined that this was a CCIS Help Desk technician error in emailing patient name and MRN. • Breach was determined to be minor in nature. Breach report was completed and submitted to CritiCall Executive Director and the investigation was completed on August 15, 2019. • CCIS Help Desk technician was coached on correct procedure/process for providing PHI to third party servicer provider (vendor) There were no additional recommendations form this investigation.
Privacy Complaints	
The number of privacy complaints received since prior review by the IPC.	There have been no privacy complaints made to HHS/CritiCall Ontario since the prior review by the IPC.
Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the IPC and with respect to each:	There have been no privacy complaints made to HHS/CritiCall Ontario since the prior review by the IPC.

- The date the complaint was received - The nature of the complaint - The date that the investigation was commenced - The date of the letter to the individual who made the privacy complaint in relation to the commencement of the investigation - The date the investigation was completed - A brief description of each recommendation made - The date each recommendation was addressed or is proposed to be addressed - The manner in which each recommendation was addressed or is proposed to be addressed and - The date of the letter to the individual who made the privacy complaint describing the nature and findings of the investigation and the measure taken in response to the complaint.	
Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the IPC and with respect to each: - The date the complaint was received - The nature of the complaint - The date of the letter to the individual who made the privacy complaint and a	There have been no privacy complaints made to HHS/CritiCall Ontario since the prior review by the IPC.

brief description of the content of the letter.	
SECURITY INDICATORS	
General Security Policies and Procedures	
The dates that the security policies and procedures were reviewed by the prescribed person since the prior review by the IPC	Since the prior IPC review, these policies and procedures have been reviewed in accordance with the annual policy review annually as follows: • • June 2017 • June 2018 • June 2019
Whether amendments were made to existing security policies and procedures as a result of the review and, if so, a list of the amended policies and procedures and, for each, a brief description of the amendment made	No amendments were made to existing policies during the review conducted in June 2017 or 2018. The following amendments were made to existing policies during the review conducted in June 2019: Edits were made to all policies to account for role changes within CritiCall Ontario for a dedicated Privacy Lead position and to HHS's organizational structure with respect to privacy operations.
Whether new security policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.	No new security policies and procedures were developed as a result of these reviews.
The dates that each amended and newly developed security policy and procedure was communicated to agents, and, for each amended and newly developed policy and procedure communicated to agents, the nature of the communication	No new policies were developed as a result of the 2017-2019 reviews. Amendments to Policies, noted above, following the 2019 review were not substantive in nature, so broad communication of the change was not specifically undertaken.

Whether the communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.	Communication materials available to the public and other stakeholders were not amended as a result of the review.
Physical Security	
The dates of audits of agents granted approval to access the premises and locations within the premises where records of PHI are retained since prior review by the IPC and for each audit - A brief description of each recommendation made - The date each recommendation was addressed or is proposed to be addressed, and - The manner in which each recommendation was addressed or is proposed to be addressed	Refer to Appendix 2- Security Audits for details
Security Audit Program	
The dates of the review of system control and audit logs since the prior review by the IPC and a general description of the findings if any, arising from the review.	Refer to Appendix 2- Security Audits for details**.**
The number and a list of security audits completed since prior review by the IPC and for each audit: - A description of the nature and type of audit completed - The date of completion - A brief description of each recommendation made - The date that each recommendation was	Refer to Appendix 2- Security Audits for details**.**

addressed or is proposed to be addressed and - The manner in which each recommendation was addressed or is expected to be addressed.	
Information Security Breaches	
The number of notifications of information security breaches or suspected breaches received since prior review by the IPC.	There have been zero notifications of information security breaches or suspected information security breaches since the last review by the IPC.
With respect to each information breach or suspected breach: - The date that the notification was received - The extent of the breach or suspected breach - The nature and extent of PHI at issue - The date that senior management was notified - The containment measures implemented - The date(s) that the containment measures were implemented - The dates that notification was provided to the HIC or any other organization - The date that the investigation was commenced - The date that the investigation was completed - A brief description of each recommendation made - The date each recommendation was addressed or is proposed to be addressed and	There have been zero notifications of information security breaches or suspected information security breaches since the last review by the IPC.

- The manner in which each recommendation was addressed or is proposed to be addressed	
HUMAN RESOURCES INDICATORS	
Privacy Training and Awareness	
The number of agents who have received and who have not received initial privacy orientation since the prior review by the IPC	All staff working at CritiCall Ontario receive initial privacy and security training when they begin working at CritiCall Ontario. 22 HHS/CritiCall staff at CritiCall and other agents with access to PHI for their CCIS job related accountabilities have attended initial and annual CCIS-role specific privacy and security orientation since initial review by the IPC.
The date of commencement of employment, contractual or other relationship for agents that have yet to receive initial privacy orientation and the scheduled date of the initial privacy orientation.	All HHS/CritiCall staff and other agents (CCSO and third party service provider vendor) have received initial CCIS privacy and security orientation.
The number of agents who have attended and who have not attended ongoing privacy training each year since the prior review by the IPC.	All agents have attended ongoing CCIS privacy and security training each year since the prior review by the IPC.
The dates and numbers of communications to agents by the prescribed person in relation to privacy since the prior review by the IPC and a brief description of each communication.	Since prior review by the IPC, the following communications have been provided to agents in relation to privacy: CCIS privacy and security policies and procedures were discussed during CCIS Role Specific Privacy and Security Training and Education sessions provided to HHS/CritiCall staff and other agents (CCSO and third party service provider staff) on the following dates: • May 15, 2018 • August 30, 2018 • September 27, 2018 • November 22, 2018

	• January 7, 2019 • April 16, 2019 • April 23, 2019 (third party service provider) • May 21, 2019 • June 10, 2019 • September 4, 2019 • October 17, 2019 (CCSO) Privacy and security are standing items on CritiCall Ontario's CCIS Operations Committee which meets minimum quarterly and which met on the following dates since prior review by the IPC: • April 27, 2018 • May 31, 2018 • July 10, 2018 • September 7, 2018 • October 25, 2018 • November 1, 2019 • December 6, 2018 • January 28, 2019 • March 13, 2019 • April 30, 2019 • May 31, 2019 • July 11, 2019 • August 15, 2019 • September 23, 2019 • October 23, 2019 • Privacy and security awareness training was provided to the CCIS third party service provider (vendor) Datavail (formerly Navantis) staff with access to PHI in the CCIS for the performance of their job related duties to support the CCIS on April 23, 2019 and attendees were required to sign off on the CCIS Confidentiality Agreement. Privacy and security awareness training was provided to CCSO staff whose job related duties support the CCIS as an agent of HHS/CritiCall on October 17, 2019 and attendees were required to sign off on the CCIS Confidentiality Agreement.

	A summary of all PHIPA Decisions issued by the IPC since prior review by the IPC were shared with all staff and Executive Council, on September 18, 2018 and May 22, 2019, respectively.
Security Training and Awareness	
The number of agents who have received and who have not received initial security orientation since the prior review by the IPC.	All agents have attended initial privacy and security training since initial prior review by the IPC.
The date of commencement of employment, contractual or other relationship for agents that have yet to receive initial security orientation and the scheduled date of the initial privacy orientation.	All CritiCall Ontario staff have received initial privacy and security orientation.
The number of agents who have attended and who have not attended ongoing security training each year since the prior review by the IPC.	All agents have attended ongoing privacy training each year since the prior review by the IPC.
The dates and numbers of communications to agents by the prescribed person in relation to information security since the prior review by the IPC and a brief description of each communication	See the answer to Indicator 4 under Privacy Training and Awareness.
Confidentiality Agreements	
The number of agents who have executed and who have not executed confidentiality agreements each year since prior review by the IPC.	100% of agents have executed confidentiality agreements since prior review by the IPC. Zero agents have not executed the Confidentiality Agreement annually.
The date of commencement of employment, contractual or other relationship for agents that have yet to execute the confidentiality agreement and the date by which the agreement must be executed.	All agents have executed Confidentiality Agreements. There are no agents who have yet to execute the Confidentiality Agreement.

Termination or Cessation	
The number of notifications received from agents since prior review by the IPC related to termination of their employment, contractual or other relationship with the prescribed person.	HHS/CritiCall has not received any notifications from agents since prior review by the IPC related to termination of their employment, contractual or other relationship with the prescribed person.
ORGANIZATIONAL INDICATORS	
Risk Management	
The dates that the corporate risk register was reviewed by the prescribed person since prior review by the IPC.	HHS/CritiCall maintains a Corporate Risk Register for the CCIS. CritiCall documents risks related to its operations, including those related to the CCIS. The CritiCall risk register in relation to the CCIS was reviewed on: • June 2018; • April 24, 2019; • October 29, 2019.
Whether amendments were made to the corporate risk register as a result of the review, and if so, a brief description of the amendments made.	No amendments to the HHS Corporate Risk Register were made related to CCIS in response to the reviews noted above.
Business Continuity and Disaster Recovery	
The dates that the business continuity and disaster recovery plan was tested since the prior review by the IPC.	The full *O8: Business Continuity and Disaster Recovery Plan*, was rolled out in 2017. CritiCall Ontario's Onsite generator (Deisel) and uninterruptable power supply (UPS) were tested on the following dates: **UPS** 2018 – Mar 08 2019 – Mar13-14 **Diesel**

	2017 – Nov 27-30 2018 – Dec 03-07 2019 – Dec 02-06 This policy was reviewed in June 2017, June 2018 and September 2019.
Whether amendments were made to the business continuity and disaster recovery plan as a result of the testing, and if so, a brief description of the amendments made.	No amendments were made as a result of testing.

Appendix 1 - Privacy Audit Program

- (Indicator 1) The dates of audits of agents granted approval to access and use personal health information since the prior review by the Information and Privacy Commissioner of Ontario and for each audit conducted:
  - A brief description of each recommendation made,
  - The date each recommendation was addressed or is proposed to be addressed, and
  - The manner in which each recommendation was addressed or is proposed to be addressed.

Audit Title	Date(s) of Audits	A brief description of each recommendation made	The date each recommendation was addressed or is proposed to be addressed	The manner in which each recommendation was addressed or is proposed to be addressed
Audit of Agents Granted Approval to Access and Use personal health information since the prior review by the Information and Privacy Commissioner of Ontario	November 2017 November 2018 October 17, 2019	No recommendations No recommendations No Recommendations	No recommendations No recommendations No recommendations	No recommendations No recommendations No recommendations

- (Indicator 2) The number and a list of all other privacy audits completed since the prior review by the Information and Privacy Commissioner of Ontario and for each audit:
  - A description of the nature and type of audit conducted,
  - The date of completion of the audit,
  - A brief description of each recommendation made,
  - , and

The manner in which each recommendation was addressed or is proposed to be addressed.

Eleven (11) Privacy Audits were completed since the Information and Privacy Commissioner of Ontario prior review of HHS/CritiCall Ontario's policies, procedures and practices and approval October 31, 2017. The Privacy Audits are documented in the following table:

# of Audits	**A description of the nature and type of audit conducted**	**Date of Audit Completion**	**A brief description of each recommendation made**	**The date each recommendation was addressed or is proposed to be addressed**	**The manner in which each recommendation was addressed or is proposed to be addressed**
3	**Determine if Privacy policies and procedures continue to align with IPC/O requirements**	May 2017 May 2018 June 2019	No recommendations No recommendations or amendments Minor revisions recommended, as detailed in body of report.	N/A. N/A See body of report for details.	N/A N/A Policies and procedures to be updated
1	**Audit of third party agreements**	January 2018 (by GRA)	No recommendations		
2	**Audit of hospital Data Sharing Agreements (Collection of PHI)**	June 2018 September 2019	No recommendations Ensure all hospitals contributing data into the CCIS enter into the approved template Data Sharing Agreement	No recommendations No recommendations	2018 – N/A 2019 – N/A
2	**Review training log to ensure all staff**	June 2018	No recommendations	No recommendations	No recommendations

	have completed Privacy/Security training	September 2019			
2	**Review of CCIS Confidentiality Agreements and Log to ensure up to date agreements have been executed for all agents with roles that require them to access, use or disclose PHI from the CCIS**	June 2018 September 2019	No recommendations No recommendations	No recommendations No recommendations	No recommendations No recommendations
1	**Review all Privacy Logs**	September 2019	No recommendations		
0	**Review all ad hoc and standard CCIS reports and scorecards to ensure aggregate/de-identified data complies with requirements from "*P24 – Policy and Procedures for De-identification and Aggregation*"**	Annual auditing of compliance in this respect was not documented from 2017-2019. However, as a matter of practice, all reports and ad-hoc score cards are audited prior to publication			

		or release under our standard quality assurance procedures			

Appendix 2 - Security Audits

- The dates of the review of system control and audit logs since the prior review by the Information and Privacy Commissioner of Ontario and a general description of the findings, if any, arising from the review of system control and audit logs.

Dates of Review of System Control and Audit Logs	A General Description of the Findings (if any)
June 16th, 2017	Vendor Access review – No findings
June 16th, 2017	User Access review – No findings
November 27th, 2017	User Access review – No findings
May 15, 2018	Account management functionality review – Identification of scenario where accounts would remain active after designated deactivation period. An application enhancement resolving the issue was completed on November 17, 2018.

- The number and a list of security audits completed since the prior review by the Information and Privacy Commissioner of Ontario and for each audit:
  - A description of the nature and type of audit conducted,
  - The date of completion of the audit,
  - A brief description of each recommendation made,
  - The date that each recommendation was addressed or is proposed to be addressed, and

The manner in which each recommendation was addressed or is expected to be addressed.

Nineteen (19) Security Audits were completed since the Information and Privacy Commissioner of Ontario prior review of HHS/CritiCall Ontario's policies, procedures and practices and approval. The Privacy Audits are documented in the following table:

# of Audits	A description of the nature and type of audit conducted	Date of Audit Completion	A brief description of each recommendation made	The date each recommendation was addressed or is proposed to be addressed	The manner in which each recommendation was addressed or is proposed to be addressed
2	**Account Access Matrix and Role Description Audit**	October 12th, 2017 September 27th, 2018	No recommendations		
1	**Review of CCIS accounts with Administrative and Support privileges**	June 16th, 2017	No recommendations		
1	**Ensure managers receive list of employees' access/roles and confirm/update as necessary**	November 2018	No recommendations		
1	**Audit access to CCIS data base to ensure only staff with CCIS responsibilities are accessing it**	June 16th, 2017	No recommendations		
2	**Account Access Matrix**	October 12th, 2017	No recommendations		

	and Role Description Audit	September 27th, 2018			
12	**Physical Security Access Audit (Data Centre)**	January 2017 April 2017 July 2017 October 2 2017 January 4 2018 April 10 2018 July 4 2018 October 4 2018 January 9 2019 April 4 2019 July 8 2019 October 2 2019	No recommendations		