Information
and Privacy
Commissioner,
Ontario, Canada

Report of the Information & Privacy Commissioner/Ontario

Review of the Hamilton Health Sciences Corporation in respect of the Critical Care Information System:

A Prescribed Person under the *Personal Health Information Protection Act*

Ann Cavoukian, Ph.D.
Commissioner
June 2014

Table of Contents

Review of the Hamilton Health Sciences Corporation In respect of the Critical Care Information System:

A Prescribed Person under the *Personal Health Information Protection Act*

The *Personal Health Information Protection Act, 2004* ("the *Act*") is a consent-based statute, meaning that persons or organizations defined as "health information custodians" may only collect, use and disclose personal health information with the consent of the individual to whom the personal health information relates, subject to limited exceptions where the *Act* permits or requires the collection, use or disclosure to be made without consent.

One such disclosure that is permitted without consent is the disclosure of personal health information to prescribed persons that compile or maintain registries of personal health information for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances pursuant to subsection 39(1)(c) of the *Act*.

Statutory Provisions Relating to the Disclosure to Prescribed Persons

Subsection 39(1)(c) of the *Act* permits health information custodians to disclose personal health information, without consent, to a prescribed person who compiles or maintains a registry of personal health information for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances. The following persons have been prescribed for purposes of subsection 39(1)(c) of the *Act:*

- Cardiac Care Network of Ontario in respect of its registry of cardiac services.
- INSCYTE (Information System for Cytology etc.) Corporation in respect of CytoBase.
- Canadian Stroke Network in respect of the Registry of the Canadian Stroke Network.
- Hamilton Health Sciences Corporation in respect of the Critical Care Information System.
- Cancer Care Ontario in respect of the Ontario Cancer Screening Registry.
- Children's Hospital of Eastern Ontario in respect of the Better Outcomes Registry and Network.
- Ontario Institute for Cancer Research in respect of the Ontario Tumour Bank.[1]

1 Persons or organizations described in subsection 3(1) of the Act that have custody or control of personal health information as a result of or in connection with performing the powers, duties or work of the person or organization.

In order for a health information custodian to be permitted to disclose personal health information to a prescribed person without consent, the prescribed person must have in place practices and procedures approved by the Information and Privacy Commissioner of Ontario ("IPC") to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information pursuant to subsection 13(2) of the Regulation 329/04 to the *Act*.

These practices and procedures must also be reviewed by the IPC every three years from the date of their initial approval, pursuant to subsection 13(2) of Regulation 329/04 to the *Act,* in order for a health information custodian to be able to continue to disclose personal health information to a prescribed person without consent, and in order for a prescribed person to be able to continue to collect, use and disclose personal health information without consent as permitted by the *Act*.

Review Process

The *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities ("Manual")* issued by the IPC in 2010, outlines the process that will be followed by the IPC in reviewing the practices and procedures implemented by prescribed persons and prescribed entities to protect the privacy of individuals whose personal information they receive and to maintain the confidentiality of that information. The *Manual* sets out the detailed obligations imposed on prescribed persons and prescribed entities arising from the review and approval process. The *Manual* requires prescribed persons and prescribed entities to have in place practices and procedures to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information. At a minimum, the prescribed person or prescribed entity must submit to the IPC the documentation described in Appendix "A" to the *Manual* containing the minimum content described in Appendix "B" to the *Manual*.

The Hamilton Health Sciences Corporation in respect of the Critical Care Information System submitted the required documentation during the period spanning July 2, 2013 to April 7, 2014. Upon receipt, the IPC conducted a detailed review of all the documentation in order to ensure that it complied with the *Manual's* requirements. Throughout and following the review, the IPC submitted comments to the Hamilton Health Sciences Corporation in respect of the Critical Care Information System describing necessary clarifications and revisions required by the IPC. Necessary clarifications and revisions were submitted by the prescribed person throughout the period of review and up until May 22, 2014.

An on-site meeting was held, on March 12, 2014, to discuss the practices and procedures implemented by the prescribed person; to provide the IPC with an opportunity to ask questions arising from the documentation provided; and to review the physical, technological and administrative security measures implemented by the prescribed person.

During the document review and on-site meeting, the Hamilton Health Sciences Corporation in respect of the Critical Care Information System was informed of the action that it was required

to take prior to the approval of its practices and procedures. Once all necessary action was taken, the IPC prepared a draft report that was submitted to the prescribed person for review and comment.

It must be emphasized that the review by the IPC was limited to personal health information collected, used and disclosed by the prescribed person pursuant to its function as a prescribed person under subsection 39(1)(c) of the *Act* and not with respect to any other role or responsibility that the prescribed person may have.

Description of the Prescribed Person

The Critical Care Information System (CCIS) was established as part of Ontario's Critical Care Strategy to ensure Ontario remains a global leader in providing critical care services and to improve access, quality and system integration in health care. The Hamilton Health Sciences Corporation ("HHS") in respect of the CCIS, operates the CCIS as part of its CritiCall Ontario Program (CritiCall). HHS's specific role is to facilitate decision-making related to resource allocation and bed management for the benefit of health care institutions across Ontario. The personal health information collected is required for assessing the effectiveness and utilization of interventions on health outcomes for patients and for assisting with individual patient triage, transfer and discharge planning activities, which facilitate or improve the provision of health care in Ontario.

The CCIS data set is comprised of personal health information collected from intensive care units of Ontario hospitals. It includes patient demographic data, data relation to admission sources, services provided, the date and times thereof, admitting diagnoses, discharge destinations, health card numbers, medical record numbers, 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.

HHS uses the information it collects through the CCIS to create aggregate level reporting on bed availability, critical care service utilization and patient outcomes data. These aggregate level reports do not contain any personal health information and are provided to the Ministry of Health and Long-Term Care, Local Health Integration Networks and hospitals to facilitate the allocation of resources and funds for improving critical care services in Ontario.

Findings of the Review

1. Privacy Documentation

General Privacy Policies, Procedures and Practices

HHS's *Privacy Policy in Respect of HHS as a Prescribed Person* describes HHS's status under the *Act* as well as its policies, procedures and practices with respect to the collection, use and disclosure of personal health information. It discusses each of the ten principles of the Canadian Standards Association's Fair Information Practices as they apply to personal health information in the custody or control of CritiCall. HHS is responsible for all data, including personal health information, in its custody or control. The Chief Executive Officer at HHS is ultimately accountable for ensuring compliance with the *Act*, its regulation, and the privacy and security policies, procedures and practices implemented. 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 *Policy* states that steps are taken to protect personal health information against theft, loss, unauthorized copying, modification or disposal.

The *Policy and Procedure for Ongoing Review of Privacy Policies, Procedures and Practices* describes the process for the development of new documents and for the revision of previously issued documents. The CritiCall Privacy Lead is responsible for initiating a review of privacy and security policies, at a minimum, on an annual basis.

Transparency

The *Policy on the Transparency of Privacy Policies, Procedure and Practices* specifies that HHS/CritiCall provides information relating to the CritiCall privacy and security policies and procedures to the public and other stakeholders through the CritiCall website. This information includes the *Privacy Policy in Respect of HHS as a Prescribed Person,* summaries of all Privacy Impact Assessments that have been conducted for the CCIS, a list of data holdings of personal health information maintained by HHS/CritiCall, information on the process for triennial reviews by the IPC and any approval letters/reports received from the IPC as a result of the reviews, any public reports submitted to the IPC, answers to Frequently Asked Questions and the contact information for the person to whom inquiries, concerns or complaints regarding HHS/CritiCall's compliance with the *Act,* its regulation and with the privacy policies, procedures or practices implemented by HHS in respect of the CCIS.

Collection of Personal Health Information

The *Policy and Procedure for the Collection of Personal Health Information* states that CritiCall only collects personal health information if the collection is permitted by the *Act* and its regulation. It also states that CritiCall collects only the minimum amount of personal health information required to achieve the purposes of the registry and does not collect personal health information if other information will serve the purpose. The CritiCall Privacy Lead has responsibility for reviewing

and approving proposals for the collection of new elements of personal health information. The Privacy Lead will confirm if the personal health information is required to enable CritiCall to fulfill its mandate, whether the collection is permitted by the *Act* and its regulation, and that any required agreements and documentation, such as Data Sharing Agreements, participation agreements, vendor contracts and statements of purpose, are executed and/or provided to the Privacy Lead prior to the collection of personal health information.

The *List of Data Holdings Containing Personal Health Information* describes the health information custodians from whom personal information is collected (i.e. participating hospitals in Ontario) and describes the data collections that are provided by the health information custodians (e.g. patient demographic information, admission and discharge data and clinical data).

The *Statements of Purpose for Data Holdings Containing Personal Health Information* describes why the CCIS was established and describes the core uses of the registry. It outlines the types of information collected and the purposes for which the information is collected i.e. to enable analysis and statistical reporting of resource requirements, utilization and capacity in relation to patient acuity and to enable evidence-based decision making to support system-wide capacity planning and targeted performance improvement initiatives. It also identifies the sources of the information.

Use of Personal Health Information

The *Policy and Procedure for Limiting Agent Access to and Use of Personal Health Information* states that CritiCall prohibits agents from accessing and using personal health information except as necessary for employment, contractual or other CCIS related responsibilities and requires agents to access and use the minimal amount of identifiable information necessary for carrying out their day-to-day employment, contractual or other responsibilities with CritiCall. All agents must complete a *CCIS Access to PHI Request Form* in order to apply for approval to access and use personal health information. The CCIS Product Manager, the CritiCall Privacy Lead, the CritiCall Manager of Information Technology and Decision Support as well as the Executive Director of CritiCall must sign off/approve the application prior to the agent obtaining access. There are five levels of access. The appropriate level of access to be granted is based on the agent's role and the purposes for which access to the personal health information is required. All approved accesses and uses of personal health information are subject to an automatic expiry after one year or sooner. The Manager, Information and Technology and Decision Support or delegate maintains the *Log of Agents Granted Approval to Access and Use Personal Health Information – Critical Care Information System*. The *Log* contains categories including the user name; the data holding; the level/type of access granted to the data holding; and the date access was granted/renewed.

Disclosure of Personal Health Information

The *Policy and Procedure for the Disclosure of Personal Health Information for Purposes other than Research* states that CritiCall discloses record-level data for purposes other than research

to other prescribed persons, prescribed entities or health data institutes for purposes related to their activities, other than research, or if required by law as well as to Medical Officers of Health for the purpose of facilitating or improving the effective provision of health care.

The *Policy and Procedure for Disclosure of Personal Health Information for Purposes other than Research* states that a prescribed person, prescribed entity or a health data institute requesting disclosure of personal health information for non-research purposes must complete a *CCIS Data Request Form (Not for Research),* which is reviewed by the CCIS Data Stewardship Committee, to determine, among other things, if the disclosure is permitted or required under the *Act* and its regulation, if the purpose for the disclosure aligns with the mandate of Critical Care Services Ontario and HHS/CritiCall, whether the personal health information is reasonably required for the purpose or whether aggregate or de-identified data would suffice, and to confirm that the amount of information requested is limited to the minimum amount reasonably required to meet the purpose. A *Data Sharing Agreement* must be executed with the prescribed person, prescribed entity or health data institute.

Individuals and organizations requesting disclosure of de-identified and/or aggregate data for non-research purposes must complete a *CCIS Data Request Form (Not for Research),* which is reviewed by the CCIS Data Stewardship Committee. The Committee undertakes a review to determine, among other things, the residual risk of re-identification. If the Committee approves the release of the de-identified or aggregate data, a *Data Sharing Agreement* must be executed.

The *Policy and Procedure for the Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements* states that CSIS permits the disclosure of personal health information for research purposes as authorized under the *Act* and its regulation. CCIS will not disclose personal health information for research purposes if other information will serve the research purpose and will not disclose more personal health information than is reasonably necessary to meet the identified research purpose. Researchers must meet the requirements for research disclosure provided in section 44 of the *Act* and its regulation. Researchers requesting disclosure of de-identified data, aggregate data or personal health information must submit a completed *CCIS Data Request Form (For Research),* a research plan and a copy of the decision of the Research Ethics Board that approved the research plan, to the CritiCall Privacy Lead for review. The CritiCall Privacy Lead reviews the form to confirm various requirements are met and documents their comments on the form. It is then forwarded to the CCIS Data Stewardship Committee for its review. The Committee considers matters, which include whether the personal health information, if any, is the minimum data set required to meet the needs of the research, whether the disclosure is aligned with Critical Care Services Ontario and HHS/CritiCall mandates, whether the *Act* permits the disclosure and whether enough detail has been provided to allow for a decision. A *Research Agreement* must be executed with researchers requesting disclosure of personal health information. A *Log of Research Agreements* is maintained by the CCIS Product Manager in collaboration with the Secretary of the CCIS Data Stewardship Committee. A *Data Sharing Agreement (for Release of Aggregate or De-identified Data)* must be executed with requesters of aggregate or de-identified data prior to an approved release for research purposes. The *Agreement* outlines the terms for the collection, use, disclosure, retention, destruction and safeguards applied to the information.

The *Template Research Agreement* contains a number of provisions including those related to the permitted uses and disclosures of personal health information; the technical, administrative and physical safeguards; the procedure to be followed in the event of a breach; audits that may be done to ensure compliance with the agreement; and the secure transfer, retention, and disposal of personal health information. It also contains schedules, which include a list of data to be provided to the researcher and a *Confidentiality Agreement* that must be signed by all persons who will have access to personal health information. All documentation pertaining to the disclosure of personal health information for research is securely retained within the HHS/CritiCall document repository.

Data Sharing Agreements

The *Policy and Procedures for the Execution of Data Sharing Agreements* requires the execution of a data sharing agreement when CritiCall is collecting personal health information from health information custodians for purposes other than research and when CCIS is disclosing personal health information for purposes other than research. Data sharing agreements are managed and executed by the Executive Director, CritiCall. A *Log of Data Sharing Agreements* is also maintained. There are two *Template Data Sharing Agreements,* one for disclosure of personal health information and one for collection of personal health information.

The *Template Data Sharing Agreements* contain provisions including those related to the use and disclosure of personal health information; the security of personal health information; data breaches; and responsibilities relating to the secure transfer, retention, and disposal of personal health information. They also contain schedules, including a list of data elements that will be provided by CritiCall or to CritiCall and a *Confidentiality Agreement* that must be signed by all persons who will have access to personal health information disclosed by CritiCall.

Agreements with Third Party Providers

The *Policy and Procedures for Executing Agreements with Third Party Service Providers in Respect of Personal Health Information* requires a written agreement to be entered into with third party service providers prior to permitting access to and use of personal health information. The *Policy* requires that no personal health information will be provided to third party service providers if other information, namely de-identified and/or aggregate information will serve the purpose and no more personal health information will be provided than is reasonably necessary to meet the purpose. The Executive Director, CritiCall is responsible for the execution of *Agreements* with third-party service providers and for retaining the signed original copies of the *Agreements* in a secure location. The Executive Director maintains the *Log of Agreements with Third Party Service Providers* and reviews it annually identifying any *Agreements* set to expire for the year ahead. Should an *Agreement* be set to expire, the Executive Director is responsible for following the 'End of Term' procedure, which includes notifying the signatory of the *Third Party Service Provider Agreement* of the date that the *Agreement* is to conclude and agreeing upon a reasonable course of action, which could include extending the agreement, entering into a new agreement or agreeing that the *Agreement* will no longer be required.

The *Template Agreement for All Third Party Service Providers* contains a number of provisions including those related to the permitted uses and disclosures of personal health information; security of personal health information; the procedure to be followed in the event of breaches; inspections that may be done to ensure compliance; and responsibilities relating to the secure transfer, retention, return and disposal of personal health information. It also contains schedules to the *Agreement* including a list of data elements to be accessed, used and/or disclosed in the course of providing specified services and a list of relevant CCIS policies and procedures with which the third party must comply. Violations of the *Agreement,* including all privacy breaches, will be subject to termination of the third party service provider agreement and all breaches must be reported at the first reasonable opportunity to the CCIS Help Desk.

Data Linkage and Data De-identification

The *Policy and Procedure for the Linkage of Records of Personal Health Information* states that HHS/CritiCall expressly prohibits the linkage of records of personal health information from the CCIS.

The *Policy and Procedures for De-identification and Aggregation* states that HHS/CritiCall prohibits the use of personal health information if other information, namely de-identified and/or aggregate information, will serve the identified purpose, and contains a definition of de-identified information, aggregate information and identifying information. Where information is aggregated, but includes information about individuals in groups of five or less, the information will not be released 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 approved by the CCIS Data Stewardship Committee. In conducting its review of the disclosure of such data, the Committee will consider the terms and conditions specified in any relevant agreements and research plans to ensure the 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 Executive Director, CritiCall 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 to identify an individual.

Privacy Impact Assessments

The *Privacy Impact Assessments Policy and Procedures* states that no changes to any existing operational, technical or information system infrastructure related to CCIS may be implemented without the completion of a Privacy Impact Assessment ("PIA"). The CritiCall Privacy Lead develops a timetable detailing when PIAs will be conducted in relation to existing data holdings and for ensuring PIAs are kept up to date. At a minimum, after a three year period has passed without changes having been made to the CCIS operations, technology and information security, the most current version of the relevant CCIS PIA will be reviewed by the CritiCall Privacy Lead to determine if it is still relevant and accurate. Completed PIAs will be forwarded to the Executive Director, CritiCall for review and then to the HHS Director of Privacy and Freedom of Information ("FOI") for feedback and approval. Final acceptance of the PIA recommendations

and final approval of the PIA report rests with the Executive Director, CritiCall. Once the recommendations are accepted, resources are assigned to each recommendation by the Executive Director. They, in turn, confirm the timelines for implementation of the PIA recommendations. The CritiCall Privacy Lead maintains a *Log of Privacy Impact Assessments,* which sets out, among other things, PIAs that have been initiated, PIAs that have been completed and PIAs that have not been undertaken and the rationale for not conducting the PIA.

Privacy Audit Program

The *Privacy Audit Policy* states that privacy audits shall be conducted on an annual basis, at minimum, to assess organizational compliance with privacy policies, procedures and practices in respect to CCIS and to assess compliance of agents permitted to access and use personal health information. Upon completion of each privacy audit, completed reports of the privacy audit findings are communicated to the Executive Director, CritiCall. A summary report of the findings of the privacy audit shall be provided to the CritiCall Executive Council, the Director, FOI, the HHS Enterprise Risk Management Committee and the Chief Executive Officer ("CEO"), HHS and the HHS Board of Directors. The Executive Director ensures that the *Log of Privacy Audits* is updated, reviews and confirms the plan for addressing the recommendations, including delegating responsibility for implementing each recommendation, and ensures that progress against the plan is tracked. The CritiCall Privacy Lead documents the completion of the audit in the *Log of Privacy Audits,* documents the draft plan for addressing the recommendations, monitors progress against the plan and brings forward reports to the Executive Director, CritiCall on a monthly basis.

Privacy Breaches, Inquiries and Complaints

The *Policy and Procedure for Privacy Breach Management* contains a definition of a privacy breach. The *Policy* requires agents to notify the Privacy Lead immediately after becoming aware of any privacy breach or suspected privacy breach. A verbal report must be followed up as soon as possible by completion of a CCIS *Incident Report Form.* The Executive Director, CritiCall or delegate immediately takes measures to contain any potential or actual breach and to prevent any additional breach by the same means. The Executive Director, CritiCall or delegate notifies the CritiCall Privacy Lead of the potential or actual breach and any containment measures taken and directs the CritiCall Privacy Lead to prepare a consolidated report on the containment measure(s). The Executive Director, CritiCall reviews the containment report and if further containment activities are required, the Executive Director will direct the appropriate parties to take the measures recommended by the CritiCall Privacy Lead.

The *Privacy Breach Management Policy* requires the health information custodian or other organization that disclosed the personal health information to CritiCall to be notified at the first reasonable opportunity whenever personal health information 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. At the discretion of the Director, Privacy and FOI, HHS, notification of the potential or actual breach shall be provided to Vice-

President Finance/Chief Financial Officer ("CFO"), HHS and the CEO, HHS. If it has been determined that a breach of personal health information has occurred and that the breach is of a material nature, the Director, Privacy and FOI, HHS, in consultation with the Executive Director, CritiCall and CFO, HHS will notify the IPC.

The *Policy and Procedure for Privacy Breach Management* states that, once containment measures are deemed to be successful, the Privacy Lead will initiate an investigation into the circumstances surrounding the potential or actual breach. The investigation may include, but is not limited to, reviews of documents, interviews with individuals who may have information about the actual or potential breach, site visits and/or inspections. The CritiCall Security Lead may also conduct an investigation, which, if it occurs, will be in accordance with the *Policy and Procedures for Information Security Breach Management*.

The Privacy Lead provides the Executive Director, CritiCall and the Director, Privacy and FOI, HHS, with a copy of the investigation findings immediately upon completion of the investigation. If it is determined that there has been a potential or actual security breach, a copy of the investigation findings will also be provided to the CritiCall Security Lead and HHS Chief Security Officer ("CSO").

On receipt of the findings of the investigation, the Executive Director, CritiCall in consultation with the CritiCall Privacy Lead and the Director, Privacy and FOI, HHS and, if required, the CritiCall Security Lead, and the HHS, CSO will determine the actions to be taken to address any outstanding issues/recommendations that have been identified through the investigation. The Executive Director, CritiCall assigns activities and associated timelines to the responsible individuals or business units. The Privacy Lead enters the activities, timelines and responsible individuals into the *Privacy Breach Log*.

The *Privacy Complaints Policy* describes CritiCall's privacy complaint management process. Information regarding the process for making a privacy complaint is available on HHS/CritiCall's web-site and in Critical Care Units participating in the CCIS. Communications materials also indicate that complaints regarding CritiCall's compliance with the *Act* and its regulations can be directed to the IPC. An individual may make a complaint or express a concern in writing or by telephone. The CritiCall Privacy Lead will determine, within two business days of receipt, whether an investigation is warranted. If the concerns cannot be addressed without an investigation, the investigation will be conducted by the Privacy Lead under the direction of the Executive Director, CritiCall in collaboration with the Director of Privacy and FOI, HHS as required. On confirmation that an investigation is required, the Privacy Lead will notify the complainant in writing in the form of a letter, acknowledging the complaint and advising that an investigation will be undertaken, providing information about the complaint investigation procedure, whether or not the complainant can expect to be contacted to provide further information, the timeframe for the investigation and the nature of the documentation that will provided at the end of the investigation.

The *Policy and Procedures for Privacy Complaints* states that the timeframe for an investigation shall not exceed twenty business days. The CritiCall Privacy Lead will summarize the investigation

findings noting any recommendation in a written report and will review the report with the Executive Director CritiCall within two business days of the completion of the investigation. The findings will be presented to the Director Privacy and FOI, HHS within two business days and it will be determined whether any other person or organization must be notified of the privacy complaint and the result of the investigation. After reviewing the findings of the investigation, the Executive Director, CritiCall in consultation with the CritiCall Privacy Lead and, if necessary, the Director of Privacy and FOI, HHS will determine the actions that must be taken to address any outstanding issues/recommendations identified through the investigation process. Within five business days after presenting the investigation findings to the Executive Director, CritiCall, the CritiCall Privacy Lead will respond to the individual who made the complaint, in writing, notifying the complainant of the investigation findings, any measures that have been or will be taken, and the complainant's right to make a complaint to the IPC. The Privacy Lead maintains the *Log of Privacy Complaint and Inquiries,* which sets out details concerning the receipt, investigation, notification and remediation of privacy complaints. The Privacy Lead monitors the progress of recommendations arising from complaints and ensures that they are addressed within the identified timelines.

The *Policy and Procedures for Privacy Inquiries* states that the CritiCall Privacy Lead responds to all privacy inquiries and notifies or escalates them to the Executive Director, CritiCall as required. Information regarding the process for making a privacy inquiry is available to the public on the HHS website and in Critical Care Units participating in the CCIS. The Privacy Lead will respond to privacy inquiries in writing, outlining the date the inquiry was received, the review by the Privacy Lead, the HHS/CritiCall response to the inquiry and how to contact the Privacy Lead for further information. The *Log of Privacy Complaints and Inquiries* describes the details of the response.

2. Security Documentation

General Security Policies and Procedures

The *Information Security Policy* defines HHS/CritiCall's business specific objectives related to information security, the HHS/CritiCall Information Security Program, and principles for information security management. It states that all agents of HHS/CritiCall must take steps that are reasonable in the circumstances to ensure that confidential information including personal health information is protected against theft, loss, unauthorized use or disclosure and that records of personal health information are protected against unauthorized copying, modification or disposal. The *Information Security Policy* establishes the role of CritiCall's Security Lead. This role includes the responsibility for establishing and overseeing the HHS/CritiCall Information Security Program. The Information Security Program consists of administrative, technical and physical safeguards that are consistent with established industry standards and practices and which are directed at effectively addressing any threats and risks identified. The Security Program requirements are documented in the form of policies and procedures including those for the ongoing review of the security policies; procedures and practices implemented, for ensuring physical security of the premises; for secure retention, transfer and disposal of records of

personal health information; to establish access control and authorization; for monitoring; for network security management; for back-up and recovery; for the acceptable use of information technology; and for information security breach management. The CSO, HHS establishes and provides leadership and direction for the Security Program, while delegating the day-to-day management of the CritiCall Security Program to the CritiCall Security Lead.

The *Policy and Procedures for Ongoing Review of Security Policies, Procedures and Practices* describes the process for the development of new documents and for the revision of previously issued documents. The CritiCall Security Lead with support from the CritiCall Manager, Information Technology and Decision Support is responsible for developing CCIS Information Security policies, procedures and practices. The CritiCall Security Lead initiates a review of every CCIS security policy, procedure and practice annually or as deemed necessary between annual review cycles to ensure consistency with any orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario; changes to the *Act* and its regulation relevant to the prescribed person; evolving industry standards and best practices; recommendations, arising from audits, privacy impact assessments and investigations into privacy and security breaches.

Physical Security

The *Policy and Procedure for Physical Security* describes the physical safeguards implemented by HHS/CritiCall to protect records of personal health information (e.g. locked doors, closed circuit TV, alarms etc.). The manager of all agents requiring access (or in the case of third parties or managers, the Executive Director, CritiCall) must apply in writing to the CritiCall Security Lead for approval to access the premises and locations within the premises where records of personal health information are retained by completing a *Request for Access to Physical Facilities Form.* The Security Lead reviews the request, logs it in the *Log of Agents with Access to the Premises of the Prescribed Person,* consults as required, determines and documents the response. Where the Security Lead approves an application for access, the Security Lead instructs the CritiCall Administrative Assistant, in writing, to provide the manager of the individual with an electronic pass key and to document the assignment of the pass key in the *Log of Agents with Access to the Premises of the Prescribed Person.*

Prior to the termination of an individual's employment or contract, in accordance with the *Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship*, the hiring manager must obtain any keys or access cards issued to the individual; notify the CCIS Help Desk to de-activate the individual's electronic pass card and access account and, if internal to HHS/CritiCall, the individual's network account. Agents must notify their manager and the CCIS Help Desk, at the first reasonable opportunity, of any theft, loss or misplacement of identification cards, access cards and/or keys. The Help Desk de-activates the access card/keys as soon as possible. On notification that an identification card or access card is stolen, misplaced or lost, the Help Desk shall confirm with the CritiCall Security Lead that the individual remains on the list of individuals with authorized access. If the person remains authorized, the Security Lead contacts the Administrative Assistant who will provide the replacement cards or pass keys

to the manager of the individual requiring access. The Security Lead documents that the card or key was replaced in the *Log of Agents with Access to the Premises of the Prescribed Person*.

Every visitor must wear a numbered badge, which identifies them as a visitor and is required to sign the Visitor Log and record their name, date and time of arrival, time of departure and the name of the agent(s) with whom they are meeting. Visitors must be accompanied by an agent at all times when in secure premises, must ensure that the identification badge is returned prior to departure and must sign out at the end of the business day. At the end of each day, the CritiCall Administrative Assistant must review the Visitor Log and check that all visitors have signed out and returned their visitor pass. If the visitor did not sign out or return their pass, the staff member escort 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 observed leaving the building or has not returned their visitor pass. The investigation will be conducted and documented in accordance with the *Policy and Procedures for Information Security Breach Management*.

Retention, Transfer and Disposal

The *Policy and Procedures for Secure Retention of Records of Personal Health Information* states that records of personal health information in electronic format are retained only as long as necessary to fulfill the purposes for which the personal health information is collected. Records of personal health information held by researchers must not be retained for a period longer than set out in the research plans. Depending on the type of personal health information, the Executive Director, CritiCall or the Manager Information Technology and Decision Support, CritiCall will have responsibility for its secure retention.

The *Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices* states that personal health information will not be stored on mobile computing equipment or accessed remotely except in very specific and exceptional circumstances. In order to retain personal health information on a mobile device or to access personal health information remotely, the agent must make a request to CritiCall Security Lead. If approval is obtained, the agent is required to adhere to specific conditions, including not remotely accessing or retaining personal health information on the mobile device if other information, such as de-identified or aggregate information, will serve the purpose and not retaining or accessing personal health information for longer than necessary to meet the identified purpose. The CritiCall Security Lead must ensure that all approvals to retain personal health information on mobile devices and to access personal health information remotely are logged.

The *Policy and Procedures for Secure Transfer of Records of Personal Health Information* states that records of personal health information must be transferred in a secure manner and using only approved methods. All CCIS data is managed electronically through a secure network. Non-electronic transfer methods are addressed in the policy to deal with circumstances that could arise very rarely wherein the CCIS could require a physical transfer in either paper-based or electronic media format. In those cases, such media would be transferred via a commercial bonded courier or by designated staff of the sender or recipient organization.

Personal health information transferred on portable media must be on an encrypted device approved by the Manager, Information Technology and Decision Support. Portable media containing personal health information must be labelled as such and should not be left unattended or publicly visible during the transfer process.

The *Policy and Procedures for Secure Disposal of Records of Personal Health Information* requires records of personal health information to be disposed of in a secure manner. Disposed of in a secure manner means that the records are destroyed in such a manner that the reconstruction of the records is not reasonably foreseeable in the circumstances. Records of personal health information in paper format are disposed of by a third party in accordance with an agreement that ensures provisions for the protection of personal health information consistent with *IPC Orders HO-001 and HO-006 and IPC Fact Sheet 10: Secure Destruction of Personal Health Information* are adhered to. Hard drives are degaussed according to industry best practice. Records of personal health information in electronic form and/or removable devices are disposed of by rendering them unusable and then discarding them. If re-use is being considered, personal health information must be erased by wiping methodology that is consistent with industry best practice.

Information Security

The *Policy and Procedure Relating to Passwords* requires agents to develop and use strong passwords when accessing the CCIS. The *Policy* describes standards for password composition, password protection and password expiry.

The *Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs* states that the access, use and modification of personal health information in the custody and control of HHS/CritiCall are monitored on an on-going basis. Audit logs capture the date and time that personal health information is accessed; the date and time of the disconnection; the nature of the disconnection; the name of the user accessing personal health information; 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 personal health information 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 Manager, Information Technology and Decision Support ensures that the audit logging facilities and log information is protected against tampering and unauthorized access and that the audit history is stored such that it may be reviewed for a period of two years from the date of each event, and that each event is retained in the logs. The Executive Director, CritiCall is responsible for ensuring that audits of the system control and audit logs are conducted by the CritiCall Security Lead. The Security Lead reviews system control and audit logs monthly and must report findings from the audit to the Executive Director, CritiCall and the HHS CSO at the earliest opportunity upon completion of the audit. On review of the findings arising from the review of system control and audit logs, the Executive Director, CritiCall, in consultation with the HHS CSO, ensures that a plan is developed to address any findings that require action, establish timelines for the findings to be addressed and ensure that the progress towards the plan is monitored and that the findings have, in fact, been addressed within the required timelines. If a finding results in the

identification of a privacy or security breach, then the CritiCall Security Lead will immediately initiate breach management activities in accordance with the *Policy and Procedures for Privacy Breach Management* or the *Policy and Procedures for Information Security Breach Management*.

The *Policy and Procedure for Patch Management* states that the Manager, Information Technology and Decision Support is accountable for the daily monitoring of patch availability by checking vendor websites or subscribing to vendor mailing lists for alerts of vulnerabilities or the release of new patches and information on specific products for all technology that has an impact on the CCIS. The CCIS support staff perform regular non-intrusive vulnerability scanning of the system and network to identify missing patches. The patch management process shall include an analysis of the available patches for verification of source and integrity and shall include determining the impact of changes to the HHS/CritiCall environment prior to recommendations of implementation of the patches. The *Policy* describes the process for the approval of patches and for the testing and implementing of patches.

The *Change Management Policy* states that requests for changes to the operational environment are subject to a thorough review and approval process. The *Policy* specifies the process related to change request submission (through the use of a *Change Form),* as well as change request review and implementation. The CCIS Product Manager is responsible for reviewing change requests, consulting with others 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. If the CCIS product manager is requesting the change, the change request is reviewed by either the CCIS Data Stewardship Committee or the CCIS Operations Committee, including the Executive Director, CritiCall. If the request is approved, the CCIS Help Desk will work with the required and affected staff to implement the change and will report back to the CCIS Operations Committee and the CritiCall Security Lead when implementation is complete.

The *Policy and Procedures for Back-up and Recovery of Records of Personal Health Information* states that all records containing personal health information in the CCIS shall be backed-up according to the schedule set out by the Manager, Information Technology and Decision Support and using the process set out in the associated procedure. The Manager, Information Technology and Decision Support determines the test schedule in accordance with the procedure for back-up and recovery. The agent responsible for back-up, testing and recovery of data shall ensure that back-ups are stored on secure devices and stored in a secure manner consistent with the requirements set out in the *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 personal health information reside on-site for a minimum of six months. After that, records shall be archived and transferred to a secure facility for storage in accordance with the *Policy and Procedure for Secure Transfer of Records of Personal Health Information.* On a monthly basis, the agent responsible for back-up, testing and recovery completes and forwards to the Manager, Information Technology and Decision Support, a back-up log report, which the Manager is to review. Should the review reveal any deviations from the schedule, the Manager is to follow-up with the agent and notify the CritiCall Security Lead. The Manager also documents information in the appropriate back-up log about records transferred to third party service providers, including the mode of transfer, confirmation of receipt and confirmation of secure

storage of the records. The Manager requires that the back-up process is tested by the agent at least quarterly, to ensure that data is available when needed, and is responsible for ensuring that the up-to-date backed-up records containing personal health information will be provided upon demand whether on-site or off-site.

The *Acceptable Use of Technology Policy* outlines the acceptable uses of information systems, technologies, equipment, resources, applications and programs regardless of whether they are owned, leased or operated by HHS/CritiCall. It sets out the uses that are prohibited without exception and those that are permitted only with prior approval.

Security Audit Program

The *Policy and Procedure in Respect of Security Audits* states that HHS/CritiCall conducts security audits which include those which assess compliance with security policies, procedures and practices; threat and risk assessments; vulnerability assessments; penetration testing; ethical hacks; and reviews of system control and audit logs. The CritiCall Security and Privacy Leads are responsible for ensuring that the security audits are completed. Security audits are conducted, at minimum, on an annual basis. The CritiCall Security Lead establishes the audit schedule on an annual basis and communicates the schedule to the individuals responsible for conducting the audits. The Security Lead maintains a log of security audits and, in collaboration with the Executive Director, CritiCall, monitors the status of the implementation of the recommendations arising from the security audits. It is the responsibility of the Executive Director, CritiCall or delegate to assign the individual responsible for addressing the recommendations and ensuring the implementation of the recommendations according to the timelines for completion. The CritiCall Security Lead maintains a *Log of Security Audits.* Completed reports of the security audit findings are immediately communicated to the Executive Director, CritiCall. A summary report of the findings of security audits is provided to the CritiCall Executive Council, the HHS Enterprise Risk Management Committee and the CEO, HHS and HHS Board of Directors.

Information Security Breaches

The *Policy and Procedure for Information and Security Breach Management* contains a definition of an information security breach. The *Policy* requires agents to notify the CCIS Help Desk as soon as reasonably possible of any information security breach or suspected security breach. When the CCIS Help Desk is notified of an actual or potential breach, the CCIS Help Desk staff member shall immediately notify the Executive Director, CritiCall or the HHS/CritiCall Administrator on-call, if the report comes in after business hours, and shall document the details provided by the reporting party, and shall provide the document to the Executive Director, CritiCall.

The Executive Director, CritiCall or delegate shall immediately take measures to contain any potential or actual breach, providing the necessary direction to any individual delegated to contain it and to prevent any additional breach by the same means, ensuring that no copies of records of personal health information have been made and that the records of personal health information are either retrieved or disposed of in a secure manner. The individuals delegated

to contain the breach shall provide regular reports to the Executive Director, CritiCall, which outline the containment measures taken including details about any disposal of data, written confirmation of the disposal, the time of disposal and the method of disposal. The containment reports will be retained in a secure section of the HHS/CritiCall document repository.

The *Policy and Procedure for Security Breach Management* requires the health information custodian or other organization that disclosed the personal health information to HHS/CritiCall to be notified at the first reasonable opportunity whenever personal health information is or is believed to be stolen, lost or accessed by unauthorized persons. The Director of Privacy and FOI, HHS or delegate will take the steps necessary to make the notifications. The Executive Director, CritiCall notifies Critical Care Service Ontario of an actual or potential breach at the time that is most appropriate and in the manner that is most appropriate given the circumstances. If, after an investigation has occurred, it has been determined that the nature of the breach is such that law enforcement should be involved, the CritiCall Executive Director, in consultation with the Executive Vice President and Chief Operating Officer, HHS, shall notify law enforcement officials. If personal health information was involved in the breach and the breach is of a material nature, the IPC will be notified of the breach.

The *Policy and Procedure for Security Breach Management* states that the CritiCall Security Lead initiates an investigation and documents the outcome of the investigation. The report shall include the circumstances surrounding the potential or actual breach; the contributing factors; the root cause; whether a breach occurred or not and whether personal health information was involved; the impact/extent of any breach; the actions taken to contain any breach; recommendations to prevent similar incidents; any notifications provided and to whom; and any follow-up actions, including dates as to when an action is required for each item. When the Executive Director, CritiCall in consultation with the CritiCall Security Lead and, if required, the CSO, HHS, the CritiCall Privacy Lead and the Director, Privacy and FOI, HHS, determines the actions that must be taken to address any outstanding issues/recommendations that have been identified through the investigation process, the Executive Director, CritiCall will assign activities and timelines associated with those activities to the responsible agents in the business units. The activities, timelines and responsible individuals shall be entered in the *Log of Information Security Breaches* maintained by the CritiCall Security Lead.

3. Human Resources Documentation

Privacy and Security Training and Awareness

The *Policy and Procedures for Privacy and Security Training and Awareness* states that agents accessing personal health information must complete an initial privacy and security orientation prior to being given access to personal health information. All agents must also attend annual privacy and security training. On completion of the corporate confidentiality agreement, the hiring manager schedules the new employee's initial privacy and security training, which is provided by the HHS Privacy and Freedom of Information Office. Attendance at this session is logged by HHS and, in the event the new employee fails to attend, the hiring manager will

be notified and training will be rescheduled. On completion of the initial privacy training, the hiring manager will schedule and the employee shall attend, role specific privacy training prior to being granted access to the CCIS and any personal health information. All HHS/CritiCall staff attends annual privacy and security training. Any role specific privacy or security 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 affected roles. The CritiCall Privacy and Security Leads maintain a *Log of Attendance at Initial Privacy and Security Orientation and Ongoing Privacy and Security Training.*

All agents of health information custodians with job-related duties that require them to access personal health information in the CCIS or to access systems that contain personal health information must participate in privacy and security training provided by their hospitals and familiarize themselves with applicable CCIS policies and procedures prior to being granted access to the CCIS and annually thereafter. Upon receipt of a request for access to CCIS, HHS/CritiCall's CCIS Training and Education Team will provide access to a standardized education package, which includes privacy and security related material including policies and procedures. Annual CCIS-related privacy and security updates will be provided to all hospitals participating in the CCIS. The CritiCall Privacy and Security Leads document that the privacy training material has been provided to each hospital on initial registration and annually.

Confidentiality Agreements

The *Execution of Confidentiality Agreements by Agents Policy* requires HHS/CritiCall agents to execute *Confidentiality Agreements* at the commencement of their employment or contractual relationship with HHS/CritiCall and prior to being given access to personal health information in the CCIS. *Confidentiality Agreements* are renewed annually on completion of annual privacy and security training. The Privacy Lead monitors and maintains the *Log of Executed Confidentiality Agreements – Critical Care Information System.*

The *Critical Care Information System Confidentiality Agreement* requires the agent to comply with the CCIS policies and procedures as well as with the *Act* and its regulation. The agent must agree not to access and use personal health information in the custody and control of HHS/CritiCall, except for the purpose of the job-related duties the agent is providing for the CCIS; not to access and use more personal health information than is reasonably necessary to meet the purpose; and not to make any unauthorized disclosures of personal health information. The agent must acknowledge having received privacy training and access to privacy policies and procedures, and must act diligently to protect personal health information. The agent must agree to report breaches to the CCIS Help Desk as soon as reasonably possible. The agent must agree to return all HHS/CritiCall property, including records of personal information and all identification cards, access cards and/or keys, upon the cessation of the relationship with HHS/CritiCall.

Responsibility for Privacy and Security

The *Job Description for Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program* and the *Job Description for Position(s) Delegated Day-to-Day Authority to Manage the Security Programs* state, respectively, that the Director, Privacy and FOI, provides counsel and guidance to the Executive Director, CritiCall and the CritiCall Privacy Lead to support the CCIS Privacy Program and that the CSO, HHS provides counsel and guidance to the Executive Director, CritiCall and the CritiCall Security Lead to support the CCIS Security Program. The Director Privacy and FOI, HHS reviews and approves all HHS/CritiCall privacy policies, procedures, practices, communication materials and role-specific privacy training material; organizes audits; receives reports of privacy impact assessments, audits, actual or potential breaches inquiries, complaint and investigations; informs the CritiCall Executive Director and the CritiCall Privacy Lead of any changes to privacy legislation or best practices that are relevant to CritiCall security operations; chairs the HHS Enterprise Risk Management Committee; and prepares quarterly reports for the Performance Monitoring Committee of the Board of Directors. The CritiCall Privacy Lead develops, implements, reviews annually and amends privacy policies, procedures and practices; moves these documents through the approval process; and logs them. The Privacy Lead provides transparency for privacy policies, procedures and practices by posting on relevant external and internal communication sites. The Privacy Lead facilitates compliance with the *Act* and its regulation and ensures agents are aware of their duties thereunder. The CritiCall Executive Director provides oversight to the CCIS Security Program and the activities of the CritiCall Security Lead, reviews and recommends to the CSO, HHS all new and revised CCIS security policies, procedures and documented practices, receives reports of all security audits, assessments, breach investigations, complaints and inquiries and reports to the CSO, HHS, and ensures that plans are in place to address all findings. The CritiCall Executive Director approves all requests for access to the CCIS, on the recommendation of the Data Stewardship Committee, as required; forwards requests for revision to CCIS data elements or research with respect to the CCIS to the appropriate CCIS Committee for review and decision; and ensures that security issues that require escalation to the CSO, HHS and others are escalated as appropriate.

Termination of Relationship

The *Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship* requires agents to securely return all property, including records of personal health information, identification cards, access cards, keys, ID badges, computers, mobile phones, pagers, USB keys and any other HHS/CritiCall related assets, upon termination or cessation of the employment or contractual relationship with HHS. Notification of termination of an employment, contractual or other relationship related to agents with access to the CCIS will be provided to the HHS/CritiCall responsible party (manager or contract signatory) as soon as it becomes known that this is the intent, or, in the case of termination for cause or other incident resulting in immediate termination, immediately. The hiring manager or delegate, prior to termination of an individual's employment or contract will notify, by e-mail, the HHS Human Resources Business Partner, the Executive Director, CritiCall, the Manager, Information Technology and Decision Support and the CritiCall Privacy Lead of the termination or cessation of employment of HHS/CritiCall staff or other agent with access to the CCIS and/or CCIS related property. The

name of the individual, title, and date/time of the termination will be provided. The Manager, Information Technology and Support will notify the CCIS Help Desk to de-activate the agent's network access account(s); de-activate the agent's access to the HHS/CritiCall premises; and log the CCIS access termination in the *Log of Agents Granted Approval to Access and Use Personal Health Information.* The hiring manager advises all employees, whose employment is ceasing, to surrender all personal health information and any HHS/CritiCall CCIS related assets. When the agent returns the property to the hiring manager, that manager will notify the Manager, Information Technology and Decision Support to check the agent's computer for the presence of personal health information and either archive any personal health information found in accordance with the *Policy and Procedure for the Secure Retention of Records of Personal Health Information* or destroy it in accordance with the *Policy and Procedure for Secure Disposal of Records of Personal Health Information;* and to check the agent's physical workplace for any portable media or printed information that may contain personal health information. Any information found in the workspace will be provided to the supervising manager to be dealt with according to the relevant policies and procedures. The hiring manager will notify all other relevant business units of the termination as required. The Manager, Information Technology and Decision Support will then complete the *Asset Inventory Return Form* for all agents terminating employment with HHS/CritiCall. Where an agent fails to return HHS/CritiCall CCIS related property, HHS/CritiCall may take further action as required. Similar procedures to those which are in place for CritiCall employees are in place in regard to the termination of third party service providers and other agents.

Discipline

The *Policy and Procedures for Discipline and Corrective Action* states that the employee's manager shall engage the Executive Director, CritiCall, who may in turn consult with the CritiCall Privacy Lead and the HHS Human Resources Business Partner, to assist with corrective action pertaining to the handling of personal health information contained within the CCIS. Depending on the seriousness of the infraction, activities may include gathering information, consulting Human Resources, interviewing witnesses, taking statements and allowing the employee an opportunity to explain his or her actions. For vendors, contractors and other non-employee agents of HHS/CritiCall, an investigation will be completed by the CritiCall Privacy Lead and/or the CritiCall Security Lead in accordance with the *Policy and Procedure for Privacy Breach Management* and/or the *Policy and Procedure for Information Security Breach Management*. The *Confidentiality Agreement,* which must be signed by all agents, states that a breach of the terms of the *Confidentiality Agreement,* HHS/CritiCall policies and procedures, and/or the provisions of the *Act* may result in disciplinary action, which can include termination of the employment or contractual relationship and fines being levied. The Executive Director, CritiCall reviews the Privacy Breach Report and/or Security Incident Report with the HHS General Counsel and confirms the recommended action to be taken, which could include retraining; a formal written or verbal warning; suspension of the employment or of the contract; discharge/termination of the contract.

4. Organizational and Other Documentation

Governance

The *Privacy Governance and Accountability Framework* states that the CEO, HHS has ultimate accountability for ensuring CritiCall's compliance with the *Act,* its regulation and the privacy policies and procedures and that he has delegated day-to-day responsibility to the Director, Privacy and FOI, HHS who reports to the CEO through the Vice President, Finance. The Executive Director, CritiCall ensures that HHS/CritiCall's agents who have access to the CCIS, comply with privacy policies, procedures and practices in respect of the CCIS. The Privacy Lead reports directly to the Executive Director, CritiCall who, in turn, reports to the Executive Vice President and Chief Operating Officer, HHS. The Chief Executive Officers of participating hospitals ensure that any of their agents who are provided access to the CCIS, comply with privacy policies, procedures and practices in respect of the CCIS. The *Security Governance and Accountability Framework* states that the CEO, HHS has ultimate accountability for the information security practices at HHS and delegates day-to-day operations of CritiCall to the Executive Director, CritiCall. The CritiCall Security Lead has day-to-day responsibility for information security matters. The CritiCall Security Lead reports to the Executive Director, CritiCall, who, in turn reports to the CEO, HHS through the Executive Vice President and Chief Operating Officer, HHS. The CSO, HHS is accountable for establishing the Enterprise Security Program and ensuring that individuals with day-to-day authority for program-based security programs have the necessary guidance and direction to discharge their security responsibilities competently, in compliance with relevant legislation and industry best practice. The CritiCall Security Lead provides reports in respect of information security and the CCIS to the CSO, HHS as set out in security policies and procedures. The CSO, HHS reports to the CEO, HHS through the Vice President Corporate Affairs and Strategy, HHS. The Executive Director, CritiCall ensures that CritiCall agents who have access to the CCIS comply with security policies, procedures and practices in respect of the CCIS and provides reports on security in respect of the CCIS on an annual basis to the HHS Board of Directors. The CritiCall Security Lead and the Manager Information Technology and Decision Support report directly to the Executive Director, CritiCall who, in turn reports to the Executive Vice President and Chief Operating Officer, HHS. The Security Contact/Officers at participating hospitals ensure that agents who are given access to the CCIS understand their hospital-specific and job-specific security roles and responsibilities. The HHS Board of Directors, Performance Monitoring Committee is the Board Committee responsible for oversight of privacy at HHS, including privacy and security related to CritiCall. The HHS Privacy Office is responsible for preparing a privacy metrics report to the HHS Executive Council on an annual basis. The CSO, HHS is responsible for preparing a report annually to the Executive Council, HHS which addresses the initiatives undertaken by the HHS/CritiCall security program including security training and the development and implementation of security policies procedures and practices. It also includes a discussion of the security audits conducted and the status of implementation of recommendations as well as information on security breaches investigated and the status of implementation of recommendations in regard thereto. The *Terms of Reference for Committees with Roles with Respect to the Privacy and Security Programs* describes the purpose, mandate, membership and reporting structure and meetings for each of the committees.

Risk Management

The *Corporate Risk Management Framework* states that, on an annual basis, the CritiCall Privacy Lead undertakes a process to identify risks related to HHS/CritiCall's ability to protect the privacy and confidentiality of the personal health information in the CCIS. The CritiCall Privacy Lead reviews risks in the following areas: power loss; communication loss; data integrity loss; data loss; accidental errors; computer virus; abuse of access privileges by agents; natural disasters; unauthorized system access by outsider; theft or destruction of computing assets; and system failure. The CritiCall Privacy Lead develops the corporate risk management framework. As well, prior to the commencement of a new project, the CritiCall Privacy Lead works with the project manager to develop a risk management plan to identify, document and manage the risks inherent in the project. The *Framework* also describes how the CritiCall Privacy Lead identifies risk, how risks are ranked and recommended risk mitigation actions. The CritiCall Privacy Lead monitors the *Corporate Risk Register* on a monthly basis. Amendments to the *Corporate Risk Register* require prior approval of the CritiCall Executive Council.

The *Policy and Procedures for Maintaining a Consolidated Log of Recommendations* requires that HHS/CritiCall maintain a consolidated and centralized log of all privacy and security related recommendations. The *Consolidated Log of Recommendations* contains recommendations arising from privacy impact assessments, privacy and security audits, threat risk assessments, investigation of privacy and security breaches and privacy complaints, and recommendations made by the IPC. The Executive Director, CritiCall is responsible for ensuring that the *Log* is updated on an on-going basis. The agent updating the *Log* shall advise the Executive Director, CritiCall and the Chair of the Executive Council, CritiCall that a new recommendation or recommendations have been added to the *Log*. On a quarterly basis or more frequently, the Chair of the Executive Council, CritiCall shall ensure that review of the *Log* is conducted by the Council to ensure recommendations have been or are being addressed in a timely fashion.

Business Continuity and Disaster Recovery

The *Business Continuity and Disaster Recovery Plan* states that the Executive Director, CritiCall ensures that the Manager, Information Technology and Decision Support develops and maintains an inventory of all critical applications and business functions and of all hardware, software, software licences, recovery media, equipment, system network diagrams, hardware configuration, software configuration settings, configuration settings for database systems and network settings for firewalls, routers, domain name servers, e-mail servers and any other mission critical components related to the CCIS. The Executive Director, CritiCall appoints a crisis management team, which is trained to handle any interruptions of or threat to the operating capabilities of HHS/CritiCall and maintains a list of agents and others who must be notified when there is an interruption or threat to the interruption of identified business processes. The Executive Director CritiCall ensures that there is a process in place for the activation of the *Business Continuity and Disaster Recovery Plan* and shall require an annual test of the *Plan*. Issues identified and actions taken during times of business interruption or threats to operating capability shall be documented in the *Crisis Management Log*. These items will be updated during regular meetings/communications until the situation is fully resolved.

Statement of IPC Approval of Practices and Procedures

The IPC is satisfied that HHS in respect of the CCIS has in place practices and procedures that sufficiently protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. Accordingly, effective June 24, 2014, the practices and procedures of the HHS in respect of the CCIS have been approved by the IPC.

In order to synchronize the timing of the IPC's review of HHS in respect of the CCIS with the reviews of other prescribed persons, this approval will remain effective until October 30, 2014. Prior to September 1, 2014, HHS should submit to the IPC a letter describing any amendments to the procedures and practices outlined in this report so that the IPC may review and approve these practices and procedures effective October 31, 2014 for a further period of three years.

Information and Privacy Commissioner
Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca