

## SWORN AFFIDAVIT

I, **Rob MacIsaac**, of the City of **Hamilton** in the province of **Ontario**, MAKE OATH AND SAY:

1. I am the **President and CEO** at **Hamilton Health Sciences Corporation (HHS)** and, as such, have knowledge of the matters to which I hereinafter depose. In swearing this affidavit, I have exercised care and diligence that would reasonably be expected of a **President and CEO** at **HHS** in these circumstances, including making due inquiries of staff and agents of **Hamilton Health Sciences Corporation in respect of the Critical Care Information System** who have more direct knowledge of the relevant matters.

2. **Hamilton Health Sciences Corporation in respect of the Critical Care Information System** has in place policies, procedures and practices to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information in accordance with its obligations under the *Personal Health Information Protection Act, 2004* and the regulations thereto, as may be amended from time to time.

3. The policies, procedures and practices implemented by **Hamilton Health Sciences Corporation in respect of the Critical Care Information System** comply with the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* that has been published by the Information and Privacy Commissioner of Ontario, as it may be amended from time to time, and subject to any Statements of Requested Exceptions attached hereto as Exhibit A.

4. Attached hereto as Exhibit B are the Privacy, Security, Human Resources and Organizational indicators of **Hamilton Health Sciences Corporation in respect of the Critical Care Information System** in compliance with the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*.



This is exhibit 'A' referred to in the affidavit of Rob MacIsaac

sworn/affirmed before me,  
this 24<sup>th</sup> day of October, 2023

19 BE

LSUC No. 57349W

**"Exhibit A"**  
**Statements of Requested Exceptions**

**TO THE**  
INFORMATION AND PRIVACY COMMISSIONER  
OF ONTARIO

**FROM**  
HAMILTON HEALTH SCIENCES/CRITICAL ONTARIO

**IN RESPECT**  
OF THE CRITICAL CARE INFORMATION SYSTEM

## “EXHIBIT A”

### Statements of Requested Exceptions


To the best of our knowledge, below are the exceptions for HHS/CritiCall with respect to compliance with the IPC Manual. HHS/CritiCall has been rebuilding the privacy and security program to establish a streamlined policy and indicator framework.

This is an ongoing and iterative process to which we welcome the IPC’s insights and feedback which will help to strengthen the privacy and security posture of the Critical Care Information System.

### Exceptions

1. Exact dates with respect to 2019, 2020 and 2021 policy reviews and audits are undocumented due to a gap in full-time privacy and security support. Pandemic-related pressures further constrained existing resources during that time period. The tracking of policy reviews and audits by specific date resumed as soon as additional and replacement resources were put in place in late 2021-2022.
2. HHS/CritiCall has conducted pen tests, however, to date, these have not included ethical hacks. Going forward, ethical hacks will be added as part of future testing and conducted at the same cadence as pen tests.
3. Through this review process, it has been identified that a formal schedule of security audits as indicated in **Table 1: Types of Audits in S15** has not been fully implemented. All audits listed in S15 will be conducted in accordance with the audit schedule and policy effective 2023 and going forward. Some work is already underway.

This is exhibit 'B' referred to in the affidavit of Rob MacIsaac  
sworn/affirmed before me,  
this 24<sup>th</sup> day of October, 2023

  
\_\_\_\_\_  
L8UC No. 57349W

**"Exhibit B"**

**Privacy, Security, Human Resources and  
Organizational Indicators**

**TO THE  
INFORMATION AND PRIVACY COMMISSIONER  
OF ONTARIO**

**FROM  
HAMILTON HEALTH SCIENCES/CRITICAL ONTARIO**

**IN RESPECT  
OF THE CRITICAL CARE INFORMATION SYSTEM**

## PRIVACY AND SECURITY INDICATORS

PRIVACY INDICATORS				
General Privacy Policies, Procedures and Practices				
Indicator:		Response:		
The dates privacy policies and procedures were reviewed since prior review by the IPC.		Since the time of last approval by the IPC in 2020, HHS/CritiCall's privacy policies and procedures have been reviewed in accordance with the annual policy review cycle as follows (see table below):		
Policy Number	Policy or Log	2020 Review Date	2021 Review Date	2022 Review Date
P1	Privacy Policy in Respect of HHS as a Prescribed Person	February through March	4/1/21	5/13/22
P2	Policy and Procedures for Ongoing Review of Privacy Policies, Procedures and Practices	February through March	February through April	2022-07-06 and 8/24/2022
P3	Policy on the Transparency of Privacy Policies, Procedure and Practices	February through March	February through April	12/5/2022 and 2022-09-29
P4	Policy and Procedure for the Collection of Personal Health Information	February through March	February through April	6/30/22
P5 & P7	List of Data Holdings and P7- Statements of Purpose for PHI Data Holdings	February through March	9/14/21	2022-02-17 and 2022-10-21
P6	Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information	February through March	February through April	9/29/22
P8	Policy and Procedure for Limiting Agent Access to and Use of Personal Health	February through March	3/1/22	2022-03-03 and 7/1/2022

	Information			
P12	Disclosure of PHI for Non-Research	February through March	4/5/21	2022-04-29 and 2022-05-12
P13	Disclosure of PHI for Research	February through March	6/3/21	6/6/22
P14	Template Research Agreement (for PHI or Quasi)	February through March	6/3/2021	6/15/22
P16	Policy and Procedures for the Execution of Data Sharing Agreements	February through March	February through April	10/13/22
P17	Template Data Sharing Agreement Disclosure	February through March	9/9/2021	3/4/22
P19	Policy and Procedures for Executing Agreements with Third Party	February through March	4/14/21	8/9/22
P20	Template Agreement for All Third Parties	February through March	February through April	10/25/22
P22	Policy and Procedures for the Linkage of Records of PHI	February through March	February through April	6/1/2022
P24	Policy and Procedures for De-Identification and Aggregation	February through March	6/4/21	5/12/2022
P25	Privacy Impact Assessment Policy and Procedures	February through March	February through April	6/30/2022
P27	Policy and Procedures In Respect of Privacy Audits	February through March	February through April	11/18/22
P29	Policy and Procedure for Privacy Breach Management	February through March	February through April	8/18/2022 and 2022-10-28
P31	Policy and Procedures for Privacy Complaints	February through March	February through April	9/29/2022
P33	Policy and Procedures for Privacy Inquiries	February through March	February through April	6/30/2022
<b>Policy Number</b>	<b>Policy or Log</b>	<b>2020 Review Date</b>	<b>2021 Review Date</b>	<b>2022 Review Date</b>

H1	Policy and Procedures for Privacy Training and Awareness	February through March	12/13/21	6/21/2022
H3	Policy and Procedure for Security Training and Awareness	February through March	February through April	12/30/2022
H5	Policy and Procedures for the Execution of Confidentiality Agreements	February through March	February through April	6/22/2022
H6	CCIS Confidentiality Agreement with Agents	February through March	6/17/21	6/21/2022
H8	Job Descriptions for Positions Delegated Day-to-Day Authority to Manage the Privacy Program	February through March	February through April	6/28/2023
H9	Job Descriptions for Positions Delegated Day-to-Day Authority to Manage the Security Program	February through March	February through April	6/28/2022
H10	Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship	February through March	February through April	7/5/2022
H11	Policy and Procedures for Discipline and Corrective Action	February through March	February through April	6/23/2022
<b>Policy Number</b>	<b>Policy or Log</b>	<b>2020 Review Date</b>	<b>2021 Review Date</b>	<b>2022 Review Date</b>
O1	Privacy Governance and Accountability Framework	February through March	4/6/21	3/4/22
O2	Security Governance and Accountability Framework	February through March	4/9/21	3/4/22
O3	Terms of Reference for Committees with Roles with Respect to the Privacy and Security Programs	February through March	February through April	4/20/22
O4	Corporate Risk Management Framework	February through March	February through April	Aug-22
O6	Policy and Procedures for Maintaining a Consolidated Log of Recommendations	February through March	February through April	8/9/22
O8	Business Continuity and Disaster Recovery Plan	February through March	February through April	5/12/22



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 2020 review cycle.

During the 2021 policy review cycle: most policies were amended with role changes and new approvers to align with organizational changes and other minor edits.

Additional amendments are as follows:

- *P7 List of Data Holdings and P5 Statements of Purpose for PHI Data Holdings* was updated to include pandemic information and a NICU statement of purpose.
- Clarification edits were made to *H1 Policy and Procedures for Privacy Training and Awareness* around the annual board report.
- Fine tuning of the Log of Attendance at Initial Privacy Orientation and Ongoing Privacy Training, Log of Attendance at Initial Security Orientation and Ongoing Security Training, and Log of Executed Confidentiality Agreements (H2, H4 & H7) to ensure better documentation around compliance with the IPC Manual (logs for privacy and security training and the confidentiality agreement).
- *01-Privacy Governance and Accountability Framework*: Updated the organizational charts and clarifications around committees and privacy governance at Hamilton Health Sciences (HHS) and CritiCall Ontario (CritiCall).
- *02-Security Governance and Accountability Framework*: Updated the organizational charts and clarifications around committees and security governance at HHS and CritiCall.
- *P12-Disclosure of PHI for Non-Research*: Updated the process for handling requests to be more precise and other clarifying edits.
- *P13-Disclosure of PHI for Research*: Updated the process for handling requests to be more precise and other clarifying edits.

During the 2022 policy review cycle most policies were amended with role changes and new approvers as applicable to align with organizational changes, and

other minor edits to style, formatting. Additional amendments made are as follows:

- *P8-Policy and Procedure for Limiting Agent Access to and Use of Personal Health Information:* Updated Admin User to SysAdmin for accuracy, minor procedural edits. Changed Audit User to Audit Officer and updated who has access (Privacy Lead). Updated the review and approval process to reflect organizational process changes.
- *P12-Disclosure of PHI for Non-Research:* Made procedural clarifications around requests for de-identified or aggregate data and other policy edits.
- *P13-Disclosure of PHI for Research:* Made procedural clarifications.
- *P24-Policy and Procedures for De-Identification and Aggregation:* Removed duplicate procedure that is in P12-process and policy edits, added in reference to P13.
- *01-Privacy Governance and Accountability Framework:* Updated who CCIS Operations Committee reports to.
- *02-Security Governance and Accountability Framework:* Updated who CCIS Operations Committee reports to.
- *03-Terms of Reference for Committees with Roles with Respect to the Privacy and Security Programs:* Updated Approvals and removed former committees, added new committees such as PSITSC to reflect current structure.
- *H3-Policy and Procedure for Security Training and Awareness:* Updated Organizational Structure.
- *H5-Policy and Procedures for the Execution of Confidentiality Agreements:* Updated Organizational Structure.
- *H8- Job Descriptions for Positions Delegated Day-to-Day Authority to Manage the Privacy Program:* Updated Organizational Structure.
- *H9-Job Descriptions for Positions Delegated Day-to-Day Authority to Manage the Security*

	<p><i>Program: Updated Organizational Structure.</i></p> <ul style="list-style-type: none"> <li>• <i>H10-Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship: Updated Organizational Structure.</i></li> <li>• <i>H11- Policy and Procedures for Discipline and Corrective Action: Updated Organizational Structure.</i></li> </ul>
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 procedures developed and implemented.	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 2020, 2021 and 2022.
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.	<p>No new privacy policies were developed as a result of the 2020- 2022 reviews.</p> <p>All policies and procedures are communicated via SharePoint and the CCIS Document Library. Policies are discussed at leadership meetings for leaders to share with their staff or at the PSITSC Committee to provide awareness. Recently CritiCall has begun emailing updated policies and procedures to all staff. Please see a list below of policies and how they were communicated in 2022.</p>

Policy Number	Policy or Log	2022 Review Date	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.
P1	Privacy Policy in Respect of HHS as a Prescribed Person	5/13/22	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access), announced at Leadership for them to bring to their teams on May 26, 2022. Email to everyone with the new policy. Email sent to all staff 2022-09-06.
P2	Policy and Procedures for Ongoing Review of Privacy Policies, Procedures and Practices	2022-07-06 and 8/24/2022	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access) on 2023-01-27

P3	Policy on the Transparency of Privacy Policies, Procedure and Practices	12/5/2022 and 2022-09-29	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access), 2023-01-27
P4	Policy and Procedure for the Collection of Personal Health Information	6/30/22	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
P5 & P7	List of Data Holdings and P7- Statements of Purpose for PHI Data Holdings	2022-02-17 and 2022-10-21	Uploaded to CCIS Policy Library, announced at PSIT January 20, 2022. Uploaded to SharePoint (all staff have access).
P6	Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information	9/29/22	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
P8	Policy and Procedure for Limiting Agent Access to and Use of Personal Health Information	2022-03-03 and 7/1/2022	Email sent to all staff 2022-10-21 in addition to shared with leaders to raise at staff meetings and discussed at PSIT meeting relevant staff.
P12	Disclosure of PHI for Non-Research	2022-04-29 and 2022-05-12	Uploaded to CCIS Policy Library, announced at Leadership for them to bring to their teams on May 26, 2022. Email to everyone with the new policy pending. Email sent to all staff 2022-09-06.
P13	Disclosure of PHI for Research	6/6/22	Uploaded to CCIS Policy Library, announced at Leadership for them to bring to their teams on May 26, 2022. Email to everyone with the new policy pending. Email sent to all staff 2022-09-06.
P14	Template Research Agreement (for PHI or Quasi)	6/15/22	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
P16	Policy and Procedures for the Execution of Data Sharing Agreements	10/13/22	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
P17	Template Data Sharing Agreement Disclosure	3/4/22	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
P19	Policy and Procedures for Executing Agreements with Third Party	8/9/22	Emailed to all staff (pending), and uploaded to the CCIS Document Library 2023-01-27
P20	Template Agreement for All Third Parties	10/25/2022	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
P22	Policy and Procedures for the Linkage of Records of PHI	6/1/2022	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).

P24	Policy and Procedures for De-Identification and Aggregation	5/12/2022	Uploaded to CCIS Policy Library, announced at Leadership for them to bring to their teams on May 26, 2022. Email to everyone with the new policy pending. Email sent to all staff 2022-09-06.
P25	Privacy Impact Assessment Policy and Procedures	6/30/2022	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
P27	Policy and Procedures In Respect of Privacy Audits	11/18/2022	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
P29	Policy and Procedure for Privacy Breach Management	8/18/2022 and 2022-10-28	Email sent to all staff 2022-11-28. Presented at EC 2023-01-26. Leaders are to review at Staff Meetings as well.
P31	Policy and Procedures for Privacy Complaints	9/29/2022	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
P33	Policy and Procedures for Privacy Inquiries	6/30/2022	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
<b>Policy Number</b>	<b>Policy or Log</b>	<b>2022 Review Date</b>	<b>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.</b>
H1	Policy and Procedures for Privacy Training and Awareness	6/21/2022	Uploaded to CCIS Policy Library, announced at Leadership for them to bring to their teams on May 26, 2022. Email to everyone with the new policy pending. Email sent to all staff 2022-09-06.
H3	Policy and Procedure for Security Training and Awareness	12/30/2022	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
H5	Policy and Procedures for the Execution of Confidentiality Agreements	6/22/2022	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
H6	CCIS Confidentiality Agreement with Agents	6/21/2022	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
H8	Job Descriptions for Positions Delegated Day-to-Day Authority to Manage the Privacy Program	6/28/2023	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
H9	Job Descriptions for Positions Delegated Day-to-Day Authority to Manage the	6/28/2022	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).

	Security Program		
H10	Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship	7/5/2022	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
H11	Policy and Procedures for Discipline and Corrective Action	6/23/2022	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
Policy Number	Policy or Log	2022 Review Date	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.
O1	Privacy Governance and Accountability Framework	3/4/22	Uploaded to CCIS Policy Library, announced at Leadership for them to bring to their teams on May 26, 2022. Email to everyone with the new policy pending. Email sent to all staff 2022-09-06.
O2	Security Governance and Accountability Framework	3/4/22	Uploaded to CCIS Policy Library, announced at Leadership for them to bring to their teams on May 26, 2022. Email to everyone with the new policy pending. Email sent to all staff 2022-09-06.
O3	Terms of Reference for Committees with Roles with Respect to the Privacy and Security Programs	4/20/22	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
O4	Corporate Risk Management Framework	Aug-22	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
O6	Policy and Procedures for Maintaining a Consolidated Log of Recommendations	8/9/22	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).
O8	Business Continuity and Disaster Recovery Plan	5/12/22	Uploaded to CCIS Policy Library and uploaded on SharePoint (all staff have access).

<p>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.</p>	<p>The following policies were updated on the CritiCall website in 2021 and 2022:</p> <ul style="list-style-type: none"> <li>• <i>P1-Privacy Policy in Respect of HHS as a Prescribed Person</i>: Updated with minor edits; and</li> <li>• <i>P7 List of Data Holdings and P5 Statements of Purpose for PHI Data Holdings</i>: Updated to include pandemic information and a NICU statement of purpose.</li> </ul>
<p><b>Collection</b></p>	
<p>The number and data holdings containing PHI maintained by the prescribed person.</p>	<p>In its capacity as a prescribed person under PHIPA, HHS/CritiCall maintains one data holding, the CCIS Data Holding (P5).</p>
<p>The number of statements of purpose developed for data holdings containing PHI.</p>	<p>The CCIS Data Holding has one table outlining the statements of purpose which is contained within <i>P7: Statements of Purpose for Data Holdings Containing Personal Health Information</i>. There are currently 14 statements of purpose in the table for 13 data element groups.</p>
<p>The number and a list of statements of purpose for data holdings containing PHI that were reviewed since the prior review by the IPC.</p>	<p>The Statement of Purpose for the CCIS Data Holding has been reviewed at least three times since the prior review by the IPC (annually).</p>
<p>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.</p>	<p>CritiCall amended <i>P5 Statements of Purpose for PHI Data Holdings</i> in 2021, to include a NICU statement of purpose.</p>
<p><b>Use</b></p>	
<p>The number of agents granted approval to access and use PHI for purposes other than research.</p>	<p>28 HHS/CritiCall agents have been granted approval to access and use the CCIS for job-related accountabilities only (not for research).</p> <p>(In addition, as of July 20, 2022, there are 4,540 agents of participating Ontario hospitals approved to access and use PHI for purposes other than research.)</p>

<p>The number of requests received for the use of PHI for research since the prior review by the IPC.</p>	<p>HHS/CritiCall has not received any requests for the use of PHI for research since the prior review by the IPC.</p>
<p>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.</p>	<p>No requests for the use of PHI for research have been granted or denied by HHS/CritiCall since the prior review by the IPC.</p>
<p><b>Disclosure</b></p>	
<p>The number of requests received for the disclosure of PHI for purposes other than research since prior review by the IPC.</p>	<p>There have been three requests for the disclosure of PHI for purposes other than research since prior review by the IPC.</p>
<p>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.</p>	<p>Three requests for the disclosure of PHI for purposes other than research have been granted since prior review by the IPC.</p>
<p>The number of requests received for the disclosure of PHI for research purposes since prior review by the IPC.</p>	<p>Six requests have been received for the disclosure of PHI for research purposes since prior review by the IPC.</p>
<p>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.</p>	<p>Two requests have been granted and three requests have been denied by HHS/CritiCall for the disclosure of PHI for research purposes since prior review by the IPC. One request was referred to its originating Hospital for review and approval.</p>
<p>The number of Research Agreements executed with researchers to whom PHI was disclosed since the prior review by the IPC.</p>	<p>Two research agreements have been executed with researchers to whom PHI was disclosed since prior review by the IPC.</p>
<p>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.</p>	<p>Two requests for de-identified/aggregate data for research and other purposes were received since prior review of the IPC.</p>



<p>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.</p>	<p>One Agreement that addresses two requests in relation to de-identified/aggregate data for research and for other purposes has been executed since prior review of the IPC.</p>
<p><b>Data Sharing Agreements</b></p>	
<p>The number of DSA's executed for the collection of PHI by the prescribed person since the prior review by the IPC.</p>	<p>Since the prior review by the IPC, 97 hospitals signed amending DSA's to address data flows and uses of the personal health information provided by participating hospitals.</p>
<p>The number of DSAs executed for the disclosure of PHI by the prescribed person since prior review by the IPC.</p>	<p>One DSA has been executed for the disclosure of PHI by CritiCall to a prescribed entity since prior review by the IPC. An amendment to that DSA is in progress.</p>
<p><b>Agreements with Third Party Service Providers</b></p>	
<p>The number of agreements executed with third party service providers with access to PHI since prior review by the IPC.</p>	<p>Since the prior review by the IPC, one new agreement has been executed with a third-party service provider (March 2021); and one amending agreement with another third-party service provider was executed (March 2021).</p>
<p><b>Data Linkage</b></p>	
<p>The number and a list of data linkages approved since the prior review by the IPC.</p>	<p>Three data linkages were approved since prior review by the IPC as follows:</p> <ol style="list-style-type: none"> <li>1. Linking with ICES Data Holdings;</li> <li>2. Ministry of Health (MOH) for data modelling for COVID-19 pandemic response; and</li> <li>3. Ontario Health for planning, monitoring and evaluation of the health care system.</li> </ol>
<p><b>Privacy Impact Assessments</b></p>	
<p>The number and a list of PIAs completed since the prior review by the IPC and for each PIA:</p> <ul style="list-style-type: none"> <li>- The data holding, information system, technology or program</li> <li>- The date of completion of</li> </ul>	<p>No net new PIA's of the CCIS have been completed since prior review of the IPC. The most recent PIA dated 2017 has been reviewed in 2020 and 2021 for continued relevancy.</p>

<p>the PIA</p> <ul style="list-style-type: none"> <li>- A brief description of each recommendation</li> <li>- The date each recommendation was addressed or is proposed to be addressed and</li> <li>- The manner in which each recommendation was addressed or is proposed to be addressed</li> </ul>	
<p>The number and a list of PIAs undertaken but not completed since the prior review by the IPC.</p>	<p>In fall 2021, CritiCall received funding to upgrade and modernize the CCIS. This project includes the engagement of a third-party vendor to provide an expert and impartial review (Privacy Impact Assessment and Threat Risk Assessment) of the AWS cloud migration and other aspects of the project. In addition, CritiCall is also ensuring that internal, preliminary reviews are conducted within the Information Technology &amp; Security and Privacy teams to ensure compliance with PHIPA, the IPC Manual for Prescribed Persons, our policies and procedures, and industry best practices.</p> <p>A new PIA is in draft and will be based on the current and future state of CCIS. This is part of an iterative process as the CCIS Modernization Project progresses with an anticipation completion in the summer of 2023</p>
<p>The number and a list of PIAs that were not undertaken but for which PIAs will be completed and the proposed date of completion.</p>	<p>Not Applicable</p>
<p>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.</p>	<p>1. A PIA was not undertaken in 2019/2020 for the addition of NICU and Pandemic data elements collected in the CCIS, as these were minor additions assessed under a Threat Risk Assessment.</p>

<p>The number and a list of PIAs reviewed since the prior review by the IPC and a brief description of the amendments made.</p>	<p>The most recent PIA dated 2017 has been reviewed in 2020 and 2021 for continued relevancy.</p>
<p><b>Privacy Audit Program</b></p>	
<p>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:</p> <ul style="list-style-type: none"> <li>• A brief description of the recommendation made</li> <li>• The date each recommendation was addressed or is proposed to be addressed and</li> <li>• The manner in which each recommendation was addressed or is proposed to be addressed</li> </ul>	<p><b>Refer to Appendix 1 - Privacy Audits for details</b></p>
<p>The number and a list of all other privacy audits completed since the prior review by the IPC and for each audit:</p> <ul style="list-style-type: none"> <li>• A description of the nature and type of audit conducted</li> <li>• The data of completion of the audit</li> <li>• A brief description of each recommendation made</li> <li>• The date each recommendation was addressed or is proposed to be addressed and</li> <li>• The manner in which each recommendation was addressed or is proposed to be addressed.</li> </ul>	<p><b>Refer to Appendix 1 - Privacy Audits for details</b></p>
<p><b>Privacy Breaches</b></p>	
<p>The number of notifications of privacy breaches or suspected privacy breaches received by the prescribed person since the prior review by the IPC.</p>	<p>None</p>

With respect to each privacy breach or suspected privacy breach: The date that the notification was received.	N/A
The extent of the privacy breach or suspected privacy breach.	N/A
Whether it was internal or external.	N/A
The nature and extent of personal health information at issue.	N/A
The date that senior management was notified.	N/A
The containment measures implemented.	N/A
The date(s) that the containment measures were implemented.	N/A
The date(s) that notification was provided to the health information custodians or any other organizations.	N/A
The date that the investigation was commenced.	N/A
The date that the investigation was completed.	N/A
A brief description of each recommendation made.	N/A
The date each recommendation was addressed or is proposed to be addressed.	N/A
The manner in which each recommendation was addressed or is proposed to be addressed.	N/A
<b>Privacy Complaints</b>	
The number of privacy complaints received since prior review by the IPC.	None

<p>Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the IPC and with respect to each:</p> <ul style="list-style-type: none"> <li>• The date the complaint was received</li> <li>• The nature of the complaint</li> <li>• The date that the investigation was commenced</li> <li>• The date of the letter to the individual who made the privacy complaint in relation to the commencement of the investigation</li> <li>• The date the investigation was completed</li> <li>• A brief description of each recommendation made</li> <li>• The date each recommendation was addressed or is proposed to be addressed</li> <li>• The manner in which each recommendation was addressed or is proposed to be addressed and</li> <li>• 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.</li> </ul>	<p>None</p>
<p>Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the IPC and with respect to each:</p> <ul style="list-style-type: none"> <li>• The date the complaint was received</li> <li>• The nature of the complaint</li> <li>• The date of the letter to the individual who made the privacy complaint and a brief description of the content of the</li> </ul>	<p>None</p>

letter.					
<b>SECURITY INDICATORS</b>					
<b>General Security Policies and Procedures</b>					
<b>Indicator:</b>		<b>Response:</b>			
The dates that the security policies and procedures were reviewed by the prescribed person since the prior review by the IPC.		Since the time of last approval by the IPC in 2020, HHS/CritiCall's security policies and procedures have been reviewed in accordance with the annual policy review cycle as follows (see table below):			
	<b>Policy Number</b>	<b>Policy or Log</b>	<b>2020 Review Dates</b>	<b>2021 Review Date</b>	<b>2022 Review Date</b>
	S1	Information Security Policy	February through March	February through April	10/4/2022
	S2	Policy and Procedures for Ongoing Review of Security Policies	February through March	February through April	5/11/22
	S3	Policy and Procedure for Physical Security	February through March	February through April	5/22/22
	S5	Policy and Procedures for Secure Retention of Records of Personal Health Information	February through March	February through April	5/24/22
	S6	Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices	February through March	February through April	5/30/22
	S7	Policy and Procedures for Secure Transfer of Records of Personal Health Information	February through March	February through April	5/25/22
	S8	Policy and Procedures for Secure Disposal of Records of Personal Health Information	February through March	February through April	5/25/22
	S9	Policy and Procedure Relating to Passwords	February through March	February through April	5/25/22

	S10	Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs	February through March	February through April	5/30/22	
	S11	Policy and Procedure for Patch Management	February through March	February through April	5/30/22	
	S12	Policy and Procedures Related to Change Management	February through March	February through April	5/30/22	
	S13	Policy and Procedures for Back-Up and Recovery of Records of Personal Health Information	February through March	February through April	5/31/22	
	S14	Policy and Procedures on the Acceptable Use of Technology	February through March	February through April	5/31/22	
	S15	Policy and Procedure In Respect of Security Audits	February through March	February through April	10/4/22	
	S17	Policy and Procedure for Information Security Breach Management	February through March	February through April	10/4/22	
<p>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</p>		<p>No amendments were made to existing policies during the 2020 and 2021 review cycle.</p> <p>During the 2022 policy review cycle the following amendments were made:</p> <ul style="list-style-type: none"> <li>All policies were reviewed and are pending minor amendments to role changes and new approvers to align with organizational changes.</li> </ul>				
<p>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.</p>		<p>No new security policies and procedures were developed as a result of these reviews.</p>				

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 security policies were developed as a result of the 2020- 2022 reviews.

All policies and procedures are communicated via SharePoint and the CCIS Document Library. Policies are discussed at leadership meetings for leaders to share with their staff or at the PSITSC Committee to provide awareness. Recently CritiCall has begun emailing updated policies and procedures to all staff. Please see a list below of policies and how they were communicated in 2022.

Policy Number	Policy or Log	2022 Review Date	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.
S1	Information Security Policy	10/4/2022	In progress – pending final review
S2	Policy and Procedures for Ongoing Review of Security Policies	5/11/2022	In progress – pending final review
S3	Policy and Procedure for Physical Security	5/22/2022	In progress – pending final review
S5	Policy and Procedures for Secure Retention of Records of Personal Health Information	5/24/2022	In progress – pending final review
S6	Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices	5/30/2022	In progress – pending final review
S7	Policy and Procedures for Secure Transfer of Records of Personal Health Information	5/25/2022	In progress – pending final review



S8	Policy and Procedures for Secure Disposal of Records of Personal Health Information	5/25/2022	In progress – pending final review
S9	Policy and Procedure Relating to Passwords	5/25/2022	In progress – pending final review
S10	Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs	5/30/2022	In progress – pending final review
S11	Policy and Procedure for Patch Management	5/30/2022	In progress – pending final review
S12	Policy and Procedures Related to Change Management	5/30/2022	In progress – pending final review
S13	Policy and Procedures for Back-Up and Recovery of Records of Personal Health Information	5/31/2022	In progress – pending final review
S14	Policy and Procedures on the Acceptable Use of Technology	5/31/2022	In progress – pending final review
S15	Policy and Procedure In Respect of Security Audits	10/4/2022	Presented to Exec Council and emailed to all staff (2022-11-03), IT leader to communicate to all IT staff at a staff meeting.
S17	Policy and Procedure for Information Security Breach Management	10/4/2022	Presented to Exec Council and emailed to all staff (2022-11-03), IT leader to communicate to all IT staff at a staff meeting.
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.	
<b>Physical Security</b>			

<p>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</p> <ul style="list-style-type: none"> <li>• A brief description of each recommendation made</li> <li>• The date each recommendation was addressed or is proposed to be addressed, and</li> <li>• The manner in which each recommendation was addressed or is proposed to be addressed</li> </ul>	<p>Refer to Appendix 2- Security Audits for details</p>
<p><b>Security Audit Program</b></p>	
<p>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.</p>	<p>Refer to Appendix 2- Security Audits for details.</p>
<p>The number and a list of security audits completed since prior review by the IPC and for each audit:</p> <ul style="list-style-type: none"> <li>• A description of the nature and type of audit completed</li> <li>• The date of completion</li> <li>• A brief description of each recommendation made</li> <li>• The date that each recommendation was addressed or is proposed to be addressed and</li> <li>• The manner in which each recommendation was addressed or is expected to be addressed.</li> </ul>	<p>Refer to Appendix 2- Security Audits for details.</p>
<p><b>Information Security Breaches</b></p>	
<p>The number of notifications of information security breaches or suspected breaches received since prior review by the IPC.</p>	<p>None</p>

<p>With respect to each information security breach or suspected information security breach:</p> <ul style="list-style-type: none"> <li>• The date that the notification was received.</li> <li>• The extent of the breach or suspected breach.</li> <li>• The nature and extent of PHI at issue.</li> <li>• The date that senior management was notified.</li> <li>• The containment measures implemented.</li> <li>• The date(s) that the containment measures were implemented.</li> <li>• The dates that notification was provided to the HIC or any other organization.</li> <li>• The date that the investigation was commenced.</li> <li>• The date that the investigation was completed.</li> <li>• A brief description of each recommendation made.</li> <li>• The date each recommendation was addressed or is proposed to be addressed; and</li> <li>• The manner in which each recommendation was addressed or is proposed to be addressed.</li> </ul>	<p>None</p>
<p><b>HUMAN RESOURCES INDICATORS</b></p>	
<p><b>Privacy Training and Awareness</b></p>	
<p>Indicator:</p>	<p>Response:</p>
<p>The number of agents who have received and who have not received initial privacy orientation since the prior review by the IPC</p>	<p>All staff working at HHS/CritiCall receive initial privacy and security orientation prior to their start date.</p> <p>73 HHS/CritiCall agents attended initial privacy and security orientation since the prior review by the IPC. Zero agents have not received initial privacy orientation.</p>

<p>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.</p>	<p>All HHS/CritiCall staff and other agents have received CCIS privacy and security orientation as part of their onboarding.</p>
<p>The number of agents who have attended and who have not attended ongoing privacy training each year since the prior review by the IPC.</p>	<p>In 2019 – 89 HHS/CritiCall agents attended ongoing (role specific) privacy and security training since the prior review by the IPC.</p> <p>In 2020 – 93 HHS/CritiCall agents attended ongoing (role specific) privacy and security training since the prior review by the IPC.</p> <p>In 2021 - 119 HHS/CritiCall agents attended ongoing (role specific) privacy and security training since the prior review by the IPC.</p> <p>From January 1, 2022 to August 2, 2022 – 4 agents completed ongoing privacy and security training. Zero agents have not attended ongoing privacy and security training.</p> <p>Zero agents have not attended ongoing CCIS privacy and security training each year since the prior review by the IPC.</p>
<p>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.</p>	<p>Since the prior review by the IPC, the following communications have been provided to agents in relation to privacy:</p> <p>CCIS privacy and security policies and procedures were reviewed during CCIS Role Specific Privacy and Security Training and Education sessions (provided to HHS/CritiCall staff and other agents, including CCSO and third-party service provider staff) on the following dates:</p> <ul style="list-style-type: none"> <li>• January 2020</li> <li>• May 2020</li> <li>• June 2020</li> <li>• September 2020</li> </ul>

- October 2020
- October 26, 2021
- November 26, 2021
- May 19, 2021
- January 12, 2022
- August 2, 2022

Privacy and security are standing items on CritiCall Ontario's CCIS Operations Committee which meets quarterly at a minimum. The following are the dates of all meetings held since the prior review by the IPC:

- April 23, 2020
- May 25, 2020
- June 29, 2020
- July 29, 2020
- September 22, 2020
- October 29, 2020
- December 14, 2020
- June 2021
- January 21, 2021
- March 02, 2021
- April 07, 2021
- May 10, 2021
- June 07, 2021
- July 15, 2021
- August 18, 2021
- February 4, 2022

Effective June 2021, many of these committee meetings were rolled into the CCIS Modernization Project discussions. These discussions are taking place several times a week and will continue until further notice.

The PSIT Steering Committee meets monthly with a small working group, addressing privacy and security matters; and quarterly with a larger cross-sectional group. The Committee has met on the following dates since its inception:

	<ul style="list-style-type: none"> <li>• 2021-06-10</li> <li>• 2021-07-08</li> <li>• 2021-07-14</li> <li>• 2021-07-26</li> <li>• 2021-09-09</li> <li>• 2021-10-14</li> <li>• 2021-12-02</li> <li>• 2022-01-20</li> <li>• 2022-03-03</li> <li>• 2022-04-07</li> <li>• 2022-05-05</li> <li>• 2022-06-16</li> <li>• 2022-07-21</li> </ul> <p>On occasion, the Privacy Lead will share media articles related to privacy with the Leadership team or all staff such as:</p> <ul style="list-style-type: none"> <li>• 2021-11-18: email sent to leadership re: Province sued over privacy breach.</li> <li>• 2022-01-28: email to all CritiCall staff sent on data privacy day with tips about privacy and data protection.</li> </ul>
<p><b>Security Training and Awareness</b></p>	
<p>The number of agents who have received and who have not received initial security orientation since the prior review by the IPC.</p>	<p>All staff working at HHS/CritiCall receive initial privacy and security orientation prior to their start date.</p> <p>73 HHS/CritiCall agents with access to PHI for their CCIS job-related accountabilities, have attended initial CCIS-role specific privacy and security orientation since the prior review by the IPC.</p>
<p>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 security orientation.</p>	<p>All HHS/CritiCall staff and other agents have received initial CCIS privacy and security orientation.</p>

<p>The number of agents who have attended and who have not attended ongoing security training each year since the prior review by the IPC.</p>	<p>In 2019 – 89 HHS/CritiCall agents attended ongoing (role specific) privacy and security training since the prior review by the IPC.</p> <p>In 2020 – 93 HHS/CritiCall agents attended ongoing (role specific) privacy and security training since the prior review by the IPC.</p> <p>In 2021 - 119 HHS/CritiCall agents attended ongoing (role specific) privacy and security training since the prior review by the IPC.</p> <p>From January 1, 2022 to August 2, 2022 – 4 agents completed ongoing privacy and security training. Zero agents have not attended ongoing privacy and security training.</p> <p>Zero agents have not attended ongoing CCIS privacy and security training each year since the prior review by the IPC.</p>
<p>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</p>	<p>See the answer to Indicator 4 under Privacy Training and Awareness.</p>
<p><b>Confidentiality Agreements</b></p>	
<p>The number of agents who have executed and who have not executed confidentiality agreements each year since prior review by the IPC.</p>	<p>73 HHS/CritiCall agents have executed confidentiality agreements since prior review by the IPC. Zero agents have not executed confidentiality agreements. The breakdown by year is as follows:</p> <p><b>2019:</b> 16 Agents have executed confidentiality agreements  <b>2020:</b> 14 Agents have executed confidentiality agreements  <b>2021:</b> 17 Agents have executed confidentiality agreements  <b>2022:</b> 26 Agents have executed confidentiality agreements</p> <p>There are no agents who have yet to execute confidentiality agreements.</p>

<p>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.</p>	<p>All agents have executed Confidentiality Agreements. There are no agents who have yet to execute the Confidentiality Agreement.</p>
<p><b>Termination or Cessation</b></p>	
<p>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.</p>	<p>HHS/CritiCall has received 26 notifications from agents since prior review by the IPC related to termination of their employment, contract or other relationship with the prescribed person.</p>
<p><b>ORGANIZATIONAL INDICATORS</b></p>	
<p><b>Risk Management</b></p>	
<p><b>Indicator:</b></p>	<p><b>Response:</b></p>
<p>The dates that the corporate risk register was reviewed by the prescribed person since prior review by the IPC.</p>	<p>HHS/CritiCall maintains a Corporate Risk Register for the CCIS.</p> <p>The CritiCall risk register, in relation to the CCIS, was reviewed on:</p> <ul style="list-style-type: none"> <li>• March 2020</li> <li>• October 2020</li> <li>• September 21, 2021</li> <li>• June 21, 2021</li> <li>• February 24, 2022</li> <li>• April 6, 2022</li> <li>• August 15, 2022</li> </ul> <p>In addition to CritiCall's Enterprise Risk Committee (ERM), the CCIS Modernization Project maintains a CCIS Risk Register and has been meeting at least weekly since June 2021.</p>
<p>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.</p>	<p>No amendments were made to the HHS Corporate Risk Register related to CCIS in response to the reviews noted above. However, additional risks are added as identified or updates to risks are made as risks are mitigated. This is an iterative process.</p>
<p><b>Business Continuity and Disaster Recovery</b></p>	



The dates that the business continuity and disaster recovery plan was tested since the prior review by the IPC.

CritiCall Ontario's Onsite generator (Diesel) and uninterruptable power supply (UPS) were tested on the following dates:

**2020:**

UPS Gamma - (Yearly) -07/21/2020

Generators - DG1-16(quarterly)

03/09/2020

06/01/2020

09/14/2020

12/07/2020

**2021:**

UPS Gamma - (Yearly) - 07/20/2021

Generators - DG1-16(quarterly)

03/08/2021

06/07/2021

09/06/2021

12/06/2021

**2022 Response:**

UPS Gamma - (Yearly) – 07/19/2022

Generators - DG1-16(quarterly)

3/07/2022 - Completed

6/06/2022 - Completed

9/06/2022 - Scheduled

12/05/2022 - Scheduled

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.

11/2021: IT updated the Rogers diagram in the BCP appendices.  
2021/11/27: Removal of Joanne Dempsey.  
2022/09/01: Replace Ryan Rebello with Maheen Shaikh.  
2023/06/16: Replace Maheen Shaikh with Ivy Dao and replace Anoshan Ariharakumaran with Jagbir Sandhu.

**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.*

<b>Dates of Audits</b>	<b>A Brief Description of each Recommendation Made</b>	<b>Date Recommendation to be Addressed</b>	<b>Manner in which each Recommendation is or will be Addressed</b>
November 2020	No Recommendations	No Recommendations	No Recommendations
November 2021	No Recommendations	No Recommendations	No Recommendations
June 2022	IT to run another audit on the SQL data (only with PHI) warehouse used by Business Innovation & Reporting team. IT to review vendor accounts access to SQL data warehouse (Database with PHI) with DXC.	October 2022	No Recommendations but will audit again in October 2022

**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.*

Thirty-Eight (38) Privacy Audits were completed since the IPC's prior review. The Privacy Audits are documented in the following table and include a high-level review of all policies and procedures for compliance with the IPC Manual, including associated logs.

Policy Number	Policy/Practice	2022 Review Date	A Brief Description of Audit Completed	Brief Description of Recommendations Made	Manner in which each Recommendation is or will be Addressed	Date Recommendation Addressed or Proposed to be Addressed
	Audit Active Provincial Users access with No PHI	1/20/2022	Audit Access	No Recommendations	N/A	N/A
	Audit Active Provincial Users with PHI	1/20/2022	Audit Access	User access and account requirements reviewed and updated accordingly.	User access was reviewed and validated to confirm that current user access is properly provisioned.	1/24/2022
	Audits of agents granted approval to the CCIS	6/16/2022	Audit Access	Run a further audit on the SQL data (only with PHI)	IT to run a further audit and analyze.	10/31/2022, Completed by 2023-03-09
P1	Privacy Policy in Respect of HHS as a Prescribed Person	5/13/22	Annual Audit	Edits, updated LHIN to Region and IPC/O to IPC, minor edits	Privacy Lead to update.	End of month, May 2022.

P2	Policy and Procedures for Ongoing Review of Privacy Policies, Procedures and Practices	2022-07-06 and 8/24/2022	Annual Audit	No Recommendations	N/A	N/A
P3	Policy on the Transparency of Privacy Policies, Procedure and Practices	5/12/22	Annual Audit	No Recommendations	N/A	N/A
P4	Policy and Procedure for the Collection of Personal Health Information	6/30/22	Annual Audit	No Recommendations	N/A	N/A
P5 & P7	List of Data Holdings and P7- Statements of Purpose for PHI Data Holdings	2/17/22	Annual Audit	Updated data elements with CCIS Product Manager	CCIS Product manager to update data elements, Privacy Lead to update policy.	End of February, 2022
P8	Policy and Procedure for Limiting Agent Access to and Use of Personal Health Information	2022-03-03 and 7/1/2022	Annual Audit	Review the Policy and Procedure with the IT Manager and Helpdesk. Admin User changed to SysAdmin for accuracy, minor procedural edits; Audit User changed to Audit Officer.	Privacy Lead to update.	End of month, July 2022. All recommendations finalized by 2022-09-08.
P12	Disclosure of PHI for Non-Research	2022-04-29 and 2022-05-12	Annual Audit	Ensure policy aligns with P24-Policy and Procedures for De-Identification and Aggregation.	Privacy Lead to update.	End of May 2022.
P13	Disclosure of PHI for Research	6/6/22	Annual Audit	Ensure policy aligns with P12-Disclosure of PHI for Non-Research and P24-Policy and Procedures for De-Identification and Aggregation.	Privacy Lead to update.	End of June 2022.



**Hamilton  
Health  
Sciences**

Template Research Agreement (for PHI or Quasi)

6/15/22

Annual Audit

No Recommendations

N/A

N/A

N/A

P14

Policy and Procedures for the Execution of Data Sharing Agreements

8/23/22

Annual Audit

In progress

Need to circle back to this one

As soon as possible

P16

Template Data Sharing Agreement Disclosure

3/4/22

Annual Audit

No Recommendations

N/A

N/A

P17

Policy and Procedures for Executing Agreements with Third Party

8/9/22

Annual Audit

Following up on DXC set to expire end of Aug (the extension).

Privacy Lead to follow up with IT Manager

End of August, 2022

P19

Template Agreement for All Third Parties

Missed in 2022

Annual Audit

In progress

Need to circle back to this one

P20

Policy and Procedures for the Linkage of Records of PHI

6/1/2022

Annual Audit

No Recommendations

N/A

N/A

P22

Policy and Procedures for De-identification and Aggregation

5/12/2022

Annual Audit

Policy requires clarifications. Remove procedural content duplicated in P12.

Privacy Lead to update.

End of May 2022.

P24

Privacy Impact Assessment Policy and Procedures

6/30/2022

Annual Audit

No Recommendations

N/A

N/A

P25

Policy and Procedures In Respect of Privacy Audits

8/9/2022

Annual Audit

Update approvers to policy.

Privacy Lead to update.

End of November 2022.

P27

Policy and Procedure for Privacy Breach Management

8/18/2022

Annual Audit

Updated to align with 2022 new draft manual

Privacy Lead to update.

End of October 2022.

P29

Policy and Procedures for Privacy Complaints

9/29/2022

Annual Audit

No Recommendations

N/A

N/A

P31

Policy and Procedures for Privacy Inquiries

6/30/2022

Annual Audit

No Recommendations

N/A

N/A

P33



**CRITICAL  
ONTARIO**

Connecting physicians, resources and care 1-800-668-HELP

Policy Number	Policy/Practice	2022 Review Date	A Brief Description of Audit Completed	Brief Description of Recommendations Made	Manner in which each Recommendation is or will be Addressed	Date Recommendation Addressed or Proposed to be Addressed
H1	Policy and Procedures for Privacy Training and Awareness	9/20/2021	Annual Audit	Policy required clarifications; staff education required updating to reflect new material, new fines as well as both general and CCIS-specific education to be updated.	Privacy Lead to update.	12/31/2021
H1	Policy and Procedures for Privacy Training and Awareness	6/21/2022	Annual Audit	Create online module	Privacy Lead to work with Client Relations Team on this.	2022-12-31 or as soon as reasonably possible
H3	Policy and Procedure for Security Training and Awareness	12/30/2022	Annual Audit	Create online module	Security Lead to work with Client Relations Team on this.	12/31/2023
H5	Policy and Procedures for the Execution of Confidentiality Agreements	6/22/2022	Annual Audit	No Recommendations	N/A	N/A
H6	CCIS Confidentiality Agreement with Agents	6/21/2022	Annual Audit	Opportunity to take this online in CCIS 2.0.	Privacy Lead to raise this with the CCIS Modernization Project Team	Proposed as part of CCIS 2.0 (Summer of 2023)
H8	Job Descriptions for Positions Delegated Day-to-Day Authority to Manage the Privacy Program	6/28/2022	Annual Audit	No Recommendations	N/A	N/A
H9	Job Descriptions for Positions Delegated Day-to-Day Authority to Manage the Security Program	6/28/2022	Annual Audit	No Recommendations	N/A	N/A





## Appendix 2 - Security Audits

### Indicator 1

▪ *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.*

The Streetsville Computing Centre (SCC) hosts the SOC1/SOC2 external audits on an annual basis.

There are three types of third-party assurance reviews:

- SOC 1 - Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (ISAE3402/SSAE 18)
- SOC 2 - Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (AT101)
- SOC 3 – Trust Services Report for Service Organizations

These audits cover all aspects based on a control environment and covers DXC IT Control Objectives:

- Physical Security
- Environmental Safeguards
- Incident Management
- Change Management
- Network Access
- Data Backup

Dates of Audits	A Brief Description of each Recommendation Made	Date Recommendation to be Addressed	Manner in which each Recommendation is or will be Addressed
August 18/19, 2020	No Recommendations	No Recommendations	No Recommendations
August 9/10, 2021	No Recommendations	No Recommendations	No Recommendations
August 19/20, 2022	No Recommendations	No Recommendations	No Recommendations

**System control audits.**

Dates of Audits	A Brief Description of each Recommendation Made	Date Recommendation to be Addressed	Manner in which each Recommendation is or will be Addressed
Monthly January 2021	Physical Security Audits Vendor Access Reviews	No Recommendations September 2021	No recommendations Vendor access to applications (CCIS, PHRS, eCeptionist) via privileged access management software finalized. Included a review of active staff and per-environment access as related to vendor duties.
Monthly	User Access Reviews (includes vendor access of environments)	None / Ongoing	External user access reviews occur on monthly basis. There is ongoing work to re-engineer some environments using PAM software and least-privilege principles.

Indicator 2

Security Audit Program

Indicator 2

*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.*

System control and audit logs are monitored 24/7 by our vendor DXC, and they are responsible to alert us if there are concerns or suspicious activity to be addressed. The table below is intended to demonstrate the reviews with vendors are taking place.

Indicator 3

- *The number and a list of security audits completed since the prior review by the IPC 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.*

Policy Number	Policy/Practice	A Brief Description of Audit Completed	2022 Review Date	Brief Description of Recommendations Made	Manner in which each Recommendation is or will be Addressed	Date Recommendation Addressed or Proposed to be Addressed
S1	Information Security Policy	Annual Audit	10/4/22	No Recommendations	N/A	N/A
S2	Policy and Procedures for Ongoing Review of Security Policies	Annual Audit	5/11/22	No Recommendations	N/A	N/A



**Hamilton  
Health  
Sciences**



**CRITICAL  
ONTARIO**

Connecting physicians, resources and care 1-800-668-HELP

S3	Policy and Procedure for Physical Security	Annual Audit	5/22/22	No Recommendations	N/A	N/A
S5	Policy and Procedures for Secure Retention of Records of Personal Health Information	Annual Audit	5/24/22	No Recommendations	N/A	N/A
S6	Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices	Annual Audit	5/30/22	No Recommendations	N/A	N/A
S7	Policy and Procedures for Secure Transfer of Records of Personal Health Information	Annual Audit	5/25/22	No Recommendations	N/A	N/A
S8	Policy and Procedures for Secure Disposal of Records of Personal Health Information	Annual Audit	5/25/22	No Recommendations	N/A	N/A
S9	Policy and Procedure Relating to Passwords	Annual Audit	5/25/22	No Recommendations	N/A	N/A
S10	Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs	Annual Audit	5/30/22	No Recommendations	N/A	N/A
S11	Policy and Procedure for Patch Management	Annual Audit	5/30/22	No Recommendations	N/A	N/A
S12	Policy and Procedures Related to Change Management	Annual Audit	5/30/22	No Recommendations	N/A	N/A
S13	Policy and Procedures for Back-Up and Recovery of Records of Personal Health Information	Annual Audit	5/31/22	No Recommendations	N/A	N/A
S14	Policy and Procedures on the Acceptable Use of Technology	Annual Audit	5/31/22	No Recommendations	N/A	N/A
S15	Policy and Procedure in Respect of Security Audits	Annual Audit	10/4/22	No Recommendations	N/A	N/A
S17	Policy and Procedure for Information Security Breach Management	Annual Audit	10/4/22	No Recommendations	N/A	N/A

# of Audits	A Description of the Nature and Type of Audit Conducted.	Date Audit Completed	Brief Description of Recommendations Made	The Date Recommendations addressed or to be Addressed	Manner in which each Recommendation is or will be Addressed
1	Account Access Matrix and Role Description Audit	July 2021	Initial audit in March 2021 noted gaps in access standardization by role. Recommended the creation of a standardized role matrix and SOP, completed in July.	July 2022	Matrix has been established. Actions undertaken in July 2022 are to review and update if needed.
1	Ensure Managers receive list of employees' roles and confirm/update access.	March 2021	As noted above with access audit, gaps were identified in role-based access. Formation of standardized access matrix was recommended.	Completed in July 2021.	A standard operating protocol with a yearly review was created. Further reviews of these indicators are recommended to proceed in accordance with that protocol.
1	Review of CCIS Accounts with Admin and Support Privileges.	June 2022	IT to run another audit on the SQL data (only with PHI) warehouse used by Business Innovation & Reporting team. IT to review vendor accounts access to SQL data warehouse	October 2022	No recommendations but will audit again in October 2022

1	A Threat Risk Assessment was conducted to review the additional NICU information now being collected from hospitals "NICU 2019 TRA".	2019-04-12	(Database with PHI) with DXC. Address gaps with CritiCall's Security Program and Associated Policies.	In progress (with assistance from third party consultant), work underway since late 2021 anticipated due date Aug 31, 2023.	To be addressed in Privacy Security Working Group (PSWG) meetings. Review vulnerability IDs and identify what's missing from current policies. Engage System Specialists for help with policies if required.
NICU 2019 TRA continued	NICU 2019 TRA continued	2019-04-12	Gaps coordinating security with service providers.	In progress, anticipated completion when new service with Datavail goes live.	Amendment to Datavail agreement that references Privacy & Security requirements to be added to the MSA.
NICU 2019 TRA continued	NICU 2019 TRA continued	2019-04-12	Gaps coordinating security with End Users.	In progress, work underway. All CCIS Data Sharing Agreements were fully executed.	Work in progress. AUP Policy to be updated in PSWG meetings. Privacy and Security to review CCIS Data sharing agreements and Terms of Use to include security requirements. CCIS PM to look into system and how users accept TOU and policies. We need annual acceptance and every time changes are made.  Privacy Lead to follow up with the hospitals that have not signed CCIS agreements.
NICU 2019 TRA continued	NICU 2019 TRA continued	2019-04-12	Increase security of PHI in the CCIS.	April 2019	PHI in the CCIS has been encrypted.

	NICU 2019 TRA continued	2019-04-12	Eliminate Form C, the CCIS registration form.	Will be eliminated with CCIS 2.0.	We have submitted for budget to have all accounts requests come through CCIS, therefore eliminating Form C.
	NICU 2019 TRA continued	2019-04-12	Increase requirements on roles and responsibilities to prevent unauthorized access to PROD/DEV/Train environments.	All user accounts will be reviewed prior to go live of the CCIS 2.0.	Prod/UAT (new roles and responsibilities have been included) released in December 2018. Train accounts were brought up for discussion in PSWG.
	NICU 2019 TRA continued	2019-04-12	Increase ability to detect, investigate or respond to security events.	New services will be included in CCIS 2.0 which will detect security events.	New jump server solution was implemented in 2019.
	NICU 2019 TRA continued	2019-04-12	Review how loss of application, system or other information service is documented.	Under review in AWS (after CCIS 2.0 is live), backups, BCP will be place.	SLAs to be reviewed in DXC agreements and added to CCIS Data Sharing agreements.
1	BCP Review	11/2021	Update Rogers diagram in appendices.	11/2021	IT updated the Rogers diagram in the BCP appendices.
1	BCP Review	2/14/2022	Review the inventory of assets.	N/A	No updates.
3	BCP Review	2021/11/27	Removal of Senior Improvement Advisor.	2021/11/27	Removal of Joanne Dempsey.
	"	2022/09/01	Update and replace BI&R Manager	2022/09/01	Replace Ryan Rebello with Maheen Shaikh.
	"	2023/06/16	Replace BI&R Manager with Interim BI&R Manager.	2023/06/16	Replace Maheen Shaikh with Ivy Dao and replace Anoshan Ariharakumaran with Jagbir Sandhu.

	BCP Review	22/09/01	Replace Help Desk Agent	22/09/01	Verified contact information.
1 Continuous Security, vulnerability reviews and assessments	Scan all servers and application for :log4j"	2021/12/10	Verify contact information. Scan all servers and application for :log4j"  SYSTEMS AFFECTED: Apache Log4j between versions 2.0 and 2.14.1.  VMware posted mitigation process to address critical vulnerability in Apache Log4j identified by CVE-2021-44228. High impact security advisory, vendor recommendation to implement mitigation as soon as possible. Urgent CR for remediation in CritiCall environment schedule for 11/12/2021 @ 20:00:00, time to implement ~ 30 min. Workaround instructions: Workaround	2021/12/11	Step 1: log4j vulnerability is set to block in the tipping point for CritiCall.  Step 2. High impact security advisory, vendor recommendation to implement mitigation as soon as possible Detailed description of Change: VCSA 6.5 Update the java-wrapper-vmon file with a text editor such as vi /usr/lib/vmware-vmon/java-wrapper-vmon At the very bottom of the file, replace the very last line with 2 new lines Original exec \$java_start_bin \$jvm_dynargs "\$@" Updated log4j_arg="- Dlog4j2.formatMsgNoLookups=true" exec \$java_start_bin \$jvm_dynargs \$log4j_arg "\$@"  Restart vCenter Services service-control --stop --all service-control --start --all



			instructions to address CVE-2021- 44228 in vCenter Server and vCenter Cloud Gateway (87081) (vmware.com)		
--	--	--	--	--	--

A TRA on the CCIS has been completed (August 2023) including a Penetration test (September 2023).