Privacy Impact Assessment
Executive Summary

Critical Care Information System (CCIS)

Confidential. Do not distribute this document without the written permission from the CritiCall Ontario Executive Director.

Modernization Project

Prepared By:	• Emily Scrivens, Privacy Specialist, PrivacyWorks • Moira Connor, Sr. Privacy Specialist, PrivacyWorks
Prepared For:	Lori Sutherland, Privacy Lead, CritiCall Ontario
Date Prepared:	**December 8, 2022**
Date Updated:	**May 5, 2023**
Version:	**V3.1 FINAL**

This privacy impact assessment (PIA) report has been prepared for CritiCall Ontario (CritiCall) as it relates to their Critical Care Information System (CCIS) and is current as of May 5, 2023. Any additions or changes to the CCIS design, or the information collected, used, stored, or disclosed by the CCIS after this date will require review by the CritiCall Privacy Lead and may require an amendment or an addendum to this PIA, or a new PIA.

This PIA report contains business confidential information and may not be duplicated or disclosed without the written permission of the CritiCall Executive Director or Privacy Lead. Information contained in the PIA has been collected directly from CritiCall, or indirectly from their public facing website. CritiCall has been provided opportunities to review the content of this PIA to ensure accuracy prior to the development of identified risks and recommended remediations.

PART 1: EXECUTIVE SUMMARY

1 EXECUTIVE SUMMARY

1.1 Background

CritiCall Ontario (CritiCall) operates the Critical Care Information System (CCIS) Prescribed Registry on behalf Hamilton Health Sciences Corporation (HHS), the "prescribed person" under Ontario's *Personal Health Information Protection Act* (PHIPA).

HHS has delegated the day-to-day operation and management of the CCIS to CritiCall, a provincial program administered by HHS and funded by the Ministry of Health and Long-Term Care (MOHLTC). For purposes of this assessment report, HHS/CritiCall will be noted as either "HHS/CritiCall" or "CritiCall".

As a key component of Ontario's Critical Care Strategy, the CCIS is used on all level 3 and 2 critical care units in Ontario to collect near-real time data on every patient. This data includes bed availability, critical care service utilization and patient outcomes which is used at the provincial level to support ongoing monitoring and effective management of the province's critical care resources.

The CCIS collects data from Hospital critical care units across Ontario and generates aggregate statistical reports on critical care services (i.e., bed availability, Admission/ Discharge/Transfer (ADT) data and Critical Care Response Team (CCRT) activity). This data is used to facilitate resource allocation and bed management decision-making.

In July 2022, PrivacyWorks Consulting was engaged by HHS/CritiCall to provide privacy and security consulting services, and to conduct in-depth security and privacy assessments related to the CCIS Modernization Project (CCIS 2.0).

Since its inception in 2007, the CCIS has relied on manual data entry and updates by Hospital staff. The CCIS 2.0 project is intended to automate, wherever possible, the collection of data directly from Hospital electronic medical record (EMR) systems (e.g., Metavision, Anzer, Quadramed, EPIC, MediTech and Cerner). This will provide more accurate and timely data to inform the ongoing development and improvement of Ontario's critical care system.

An additional and foundational component of this project is moving from the current server-based technical infrastructure for both the CCIS and CritiCall's Provincial Hospital Resource System (PHRS) to a secure Cloud, Amazon Web Services (AWS).

This privacy impact assessment (PIA) is a key deliverable of the assignment and was developed based on our assessment of CCIS compliance with privacy law in Ontario, privacy by design (PbD) principles, and privacy best practices.

This CCIS assessment includes both the current state (CCIS 1.0) and future state (CCIS 2.0). The CCIS 2.0 portion of the assessment is conditional until finalized design documentation can be provided, and the system available for testing.

1.2 Objective

The purpose of this PIA is to provide information on the CCIS and its privacy safeguards and controls, and to provide recommendations on how to mediate any identified gaps in meeting regulatory requirements, and/or alignment with PbD and/or general privacy principles.

In summary, the objective of this PIA is to provide CritiCall with:

- a point-in-time assessment of CCIS 1.0 and CCIS 2.0 privacy safeguards and controls; and
- recommendations on how to mediate any identified gaps in meeting regulatory requirements, and/or alignment with PbD and/or general privacy principles.

1.3 Scope

The scope of this assessment is limited to:

- a general review of CCIS 1.0;
- a review of the CCIS migration to the AWS cloud, hosted in an AWS Canadian datacentre;
- migration of PHRS data to the AWS cloud, and HL7 integration interfaces; and
- the separation of the repatriation data from the PHRS, to be hosted in the AWS cloud as the Repatriation Tool.

1.3.1 Out of Scope

This privacy assessment does not include an assessment of:

- the CritiCall Call Centre (eCeptionist);
- the privacy safeguards and controls of Hospitals participating in the CCIS;
- the AWS cloud security, the architectural solution design, or any security functionality or technology. These will be included in the standalone *Security Threat Risk Assessment* (STRA) document;
- the PHRS, but may describe any interaction with CCIS;
- current disaster recovery plans (DPRs), and
- the Repatriation Tool (but may discuss the separation of repatriation data from the PHRS).

1.4 Assumptions

This PIA is based on information made available to the authors during the period from July 2022 to February 16, 2023. Any CCIS 2.0 design decisions made after February 16, 2023, that impacts CCIS 2.0's collection, use, transfer, storage, and disclosure of personal information is not included in this assessment, and should be included in a subsequent addendum.

1.5 Approach

The following diagram illustrates the key steps, and timelines, in the development of the PIA. The timeline for requesting PIA sign-off was moved to early March to allow sufficient time for project team review feedback, and addition on new information.

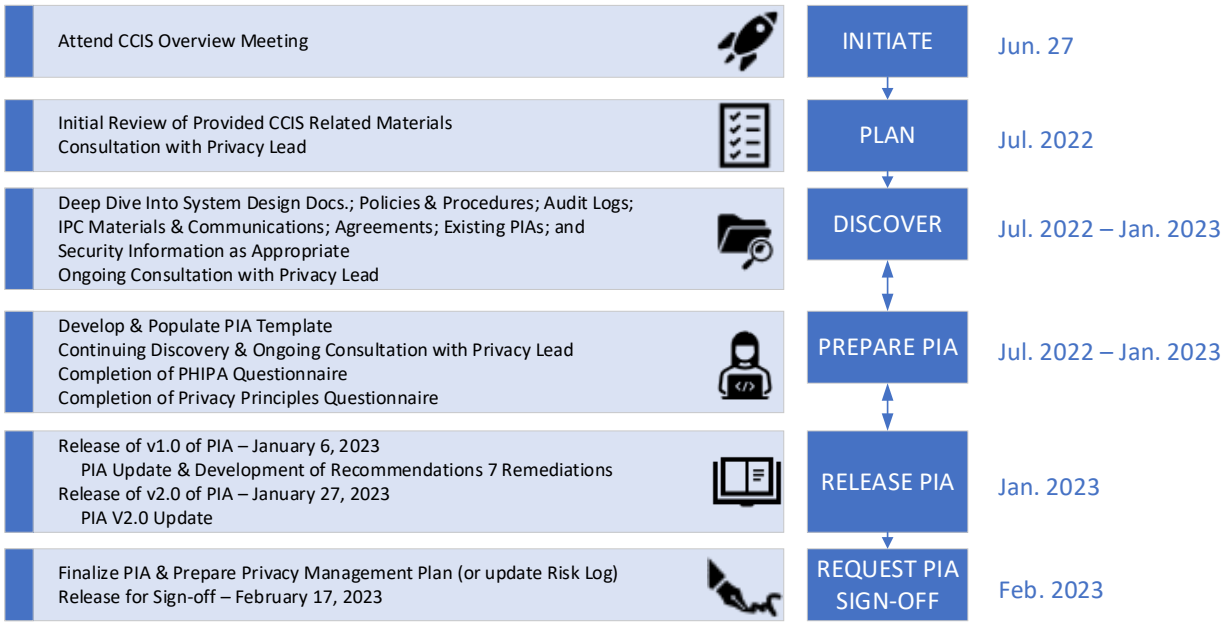

Figure 1 - PIA Approach & Timeline

1.6 Findings

CritiCall has developed and implemented various controls to ensure adequate protection of personal information (including PHI) within its custody and/or control. Comprehensive policies and procedures are in place to govern the collection, use, storage, and destruction of personal information, and staff are required to complete privacy training to ensure their knowledge and understanding of their privacy obligations. Additionally, physical, and technical security controls have been put in place to protect personal information from unauthorized access or disclosure.

However, as noted in the Risks, Recommendations & Priorities section of this PIA (Risks, Recommendations & Priorities), twelve recommendations should be addressed to further improve CritiCall's privacy protection posture. These recommendations have been prioritized based on the likelihood that a risk could be realized, and the impact should that risk occur.

It is recommended that the identified risks be addressed to a level satisfactory to the HHS/CritiCall Executive Director, Privacy Lead, the Security Lead, within the timeline indicated in the following table.

Risk Rating	Risk Number	Ideally to be addressed:
High	1, 2, 3	Within three months.
Medium	4, 5, 6, 7, 8, 9	Within one year.
Low	10, 11, 12	Within next 3-year IPC review cycle.