CII PIA Summary & Expedited PIA Instructions

CII participant's guide to the Privacy Impact Assessment (PIA) submission and Summary of the Community Information Integration (CII) PIA and addendums for the Central Patient Attachment Registry (CPAR) and eNotification of ADT Events

Purpose

The purpose of this document is to outline the PIA process for CII participants and to summarize the PIA for CII and addendums prepared by Primary & Preventative Health Services (PPHS) on behalf of participating custodians. The intended audience is custodians who have already met the administrative and technical requirements to participate in the CII initiative and who are now preparing a PIA submission.

NOTE There are other basic technical and administrative requirements that custodians must meet to participate in the CII initiative, which are outlined in the frequently asked questions documents.

Support Contact Information

eHealth Services Provider Support assists participants in meeting the requirements to participate in the CII initiative.

1-855-643-8649 (toll free)

Email: eHealthProviderSupport@gov.ab.ca

PIA process for custodians participating in CII

In CII, each participant's Electronic Medical Record (EMR) system will be modified to create new disclosures of health information to the Alberta Electronic Health Record (EHR), also known as Alberta Netcare. This change triggers the PIA requirement. Because all participants in CII are making the same change, PPHS prepared a PIA for CII on their behalf and submitted it to the OIPC for review and comment. It was accepted in August, 2017 (OIPC Reference #005962).

Since the original CII PIA was accepted, PPHS has submitted two addendums:

Addendum 1: CPAR submissions through the CII hub (OIPC File reference # 009517).

Addendum 2: Provision of eNotifications and Admission, Discharge and Transfer Events via CII Hub and CPAR. (OIPC File reference 009517).

In lieu of submitting their own PIA for CII and related addendums, participants may leverage their past PIA work and endorse the PPHS PIA for CII and/or the addendums for CPAR and eNotifications.

Eligibility to use CII PIA endorsement process

Custodians must meet the following pre-requisites to use this PIA endorsement process for CII:

- Establish policies and procedures that facilitate implementation of the HIA, as required by section 63 of the HIA. These policies must include the custodian's organizational management structure that supports HIA compliance.
- Have a PIA for their EMR that has been accepted by the OIPC and that reflects the current technical and administrative environment at their practice.

Endorsing PPHS' PIA for CII/CPAR

Under this process, custodians review the CII PIA and addendums summary (this document and/or PPHS' CII PIA and addendums and submit the following:

A letter endorsing the PPHS PIA for CII (referencing OIPC PIA files 005962, 009517 and that includes an acknowledgement that the custodian:

1. Has reviewed and met all of the privacy and security requirements described within the CII PIA and applicable addendums.
   a) Understands their responsibilities and obligations when participating in CII.
   b) Understands that they are responsible for submitting a PIA amendment to the OIPC if there is a change to their own HIA policies.

c) Acknowledges that they are solely responsible for PIAs related to any other EHR systems in their custody or control.

2 OIPC file reference to the custodian's previously accepted EMR PIA that contains the custodian's policies and procedures that facilitate implementation of the HIA, or a current copy of the custodian's policies and procedures.

Background: PIA Requirements

Under the Health Information Act (HIA), custodians must submit a PIA to the Office of the Information and Privacy Commissioner (OIPC) of Alberta before implementing administrative practices and information systems that collect, use or disclosure individually identifying health information. A PIA must also be submitted before making changes to those practices or systems.

The PIA is a due diligence tool for identifying and addressing privacy risks that may occur within a practice or information system. Each PIA a custodian prepares focuses on a particular project or initiative and includes an examination of organizational privacy practices. This includes the custodian's policies and procedures that support HIA compliance.

The OIPC reviews and comments on PIAs and considers whether the custodian has taken reasonable measures to protect privacy. The OIPC has developed PIA Requirements to help custodians complete PIAs. According to the Requirements, a properly completed PIA consists of five sections:

Section A	Project Summary
Section B	Organizational Privacy Management
Section C	Project Privacy Analysis
Section D	Project Privacy Risk Mitigation
Section E	Policy & Procedures

Summary of the CII PIA

The following is a summary of key information contained within the CII PIA. It is being provided to allow custodians to endorse PPHS' CII PIA. Custodians are responsible and accountable for ensuring that they meet all of the privacy and security requirements described within the CII PIA and addendums. It is therefore important that custodians understand fully the commitments and responsibilities they undertake and accept when they make their submission to the OIPC.

The CII PIA and addendums follow the OIPC PIA Requirements format described above. Information from each of the five sections, relevant to the custodian, has been provided below.

Section A – Project Summary

Community Information Integration (CII)

CII has three objectives:

1. To collect primary care data and specialist consult reports from community-based physician clinics;
2. To present this data to other health care providers through Alberta Netcare; and
3. To make the data available to PPHS for health system management.

Data Elements

The community based primary care report template of 84 data elements is called a Community Encounter Digest (CED). Specialist reports are narrative and in PDF. Both can be viewed by authorized users through the Alberta Netcare Portal (ANP).

Data Flow

1 Community physicians and affiliates enter health information and specialist consult reports into their EMR.

2 The EMR vendor extracts health information from the community physician's EMR and sends them to the CII Hub (integration engine). Consult reports are sent to the CII Hub by the specialist or authorized staff.

3 Patient registration information is verified.

4 Validated health information is formatted into a Community Encounter Digest for each patient.

5 New records in the CII Hub are analyzed by PPHS and validated records are submitted to Alberta Netcare.

Safeguards

The project uses a data centre managed by Orion Health (appointed as an information manager of PPHS) in Ontario. The data centre must meet high standards and Orion Health must demonstrate its ability to meet the standards through use of third-party penetration testing and vulnerability assessments.

Data moving between systems is securely transferred. Access to health information is restricted and monitored and access is audited.

Addendum 1: CPAR

Administered by Alberta Blue Cross (ABC), CPAR supports two business functions:

1. Identification of patient-provider attachments through the administration of panels. This supports continuity of care between a single provider and patient.
2. Identification of patient-program affiliations through the administration of rosters. This supports the implementation of alternative compensation models.

Data Elements

CPAR collects patient information, panel affiliation information, roster affiliation information, provider information and administration information for panel setup, panel administrator, roster administrator and program owner.

Data Flow

Manual process:

1 Panel files can be uploaded to CPAR through the CPAR user portal.

2 CPAR sends the file to CII for validation, and receives the validated patient attachments back for uploading into the Registry.

Automated process:

1 EMRs with CII functionality send panel information directly to CII for validation.

2 CPAR receives the validated patient attachments for uploading into the Registry.

Safeguards

The CPAR system resides in a data centre operated by ABC (as an information manager for PPHS). The ABC data centre security provisions and practices were reviewed by PPHS. ABC is contractually required to meet PPHS standards for privacy and security. All data transferred between CPAR and PPHS use encrypted protocols.

Addendum 2: eNotification of Admission, Discharge and Transfer Events

Information about a patient's interactions with the hospital system is not automatically published to the patient's family physician or other primary provider. ADT events are currently collected from AHS facilities and made available for viewing through the Alberta Netcare Portal (ANP). It is neither practical nor feasible for primary providers to search ANP each day for every patient on their panel in order to see if any ADT events have occurred.

As a result, the primary provider is often unaware that a patient has visited a hospital or emergency department unless / until the patient comes in to the community physician clinic for follow-up care. This current-state poses some significant risks to patient care.

CII will address these current-state problems by publishing automated eNotifications of key ADT events to the primary provider's EMR.

Data Flow

1 AHS sends a copy of all ADT event messages to the CII Hub.

2 CII Hub identifies the patient from the message and queries CPAR to determine if the patient's primary care provider is known. If known, then CPAR responds with the provider information.

3 CII Hub identifies which EMR system the provider uses and sends the ADT eNotifications to the EMR vendor's queue for pick up.

4 EMR vendor delivers ADT eNotifications to the provider's EMR.

5 CII Hub sends processing counts and error logs to the PPHS data repository.

Safeguards

The project uses a data centre managed by Orion Health (appointed as an information manager of PPHS) in Ontario. The data centre must meet high standards and Orion Health must demonstrate its ability to meet the standards through use of third-party penetration testing and vulnerability assessments.

Data moving between systems is securely transferred. Access to health information is restricted and monitored and access is audited.

Section B – Organization Privacy Management

PPHS has established a governance structure that (among other things) ensures that collection, use and disclosure of health information in the CII initiative complies with the HIA. This governance structure includes members of health professional colleges and associations and reports to the Health Information Data Governance Committee (HIDGC). The HIDGC provides advice to the Minister of Health regarding the Alberta EHR, known as Alberta Netcare. CII is an Alberta Netcare initiative.

Participating custodians must establish their own policies and procedures to facilitate implementation of the HIA in their practices. Custodians will reference previously submitted policies and procedures or attach their policies and procedures to their endorsement of PPHS' CII PIA.

Section C – Privacy Analysis

Custodians will disclose health information from their EMR systems to PPHS under the authority of the HIA, which permits custodians to disclose health information to PPHS as part of its mandate to manage Alberta Netcare and to fulfill its role in managing the provincial health system. The HIA permits participating custodians to make this information available via Alberta Netcare to other health care providers with a need to know to provide health services to patients. PPHS will also use this information within its data analytics systems to perform such activities as planning, quality improvement and health system management.

The above disclosures and subsequent uses of health information are authorized under the HIA by direct legislative authority, rather than patient consent.

However, custodians must notify patients about the purposes for which their health information will be used. Further, custodians must only collect, use and disclose the minimum amount of health information essential to meet the intended purpose and consider any wishes expressed by patients to limit disclosure. PPHS has developed a policy on handling expressed wishes and provided guidance for custodians when considering expressed wishes in relation to the CII initiative.

New health information will be validated to ensure records are complete and are attached to the correct patient.

PPHS has contracted with Orion Health to store and integrate health information for the CII initiative. Orion Health is considered PPHS' Information Manager under the HIA. As such, PPHS and Orion Health have entered into an HIA- required Information Manager Agreement to govern this arrangement, which ensures that PPHS maintains control over the health information in question.

Participating custodians must have HIA-compliant Information Manager Agreements with their EMR vendors in order to participate in CII. These agreements authorize EMR vendors to disclose CII data to PPHS via Orion Health.

Section D - Project Privacy Risk Mitigation

PPHS has submitted PIAs for the CII, CPAR and eNotification initiatives to the Office of the Information and Privacy Commissioner of Alberta (OIPC).

This overview provides a summary of the most pertinent security and risk mitigation aspects of the above systems.

CII

Access Controls

Access by employees of the CII Hub vendor and EMR vendors is limited to those with specific job responsibilities related to the CII initiative. Access controls and audit logs meet the provincial logging

and audit standard (PLAS). Access is logged and audit logs are reviewed on a regular basis.

Privacy Risks

- **Risk 1**: **Unauthorized use of information by internal or authorized parties**

  Mitigation: Employees and contractors are bound by employment oaths and legal agreements to maintain confidentiality. Non-compliance may result in fines or other penalties.

- **Risk 2**: **Unauthorized collection, use or disclosure by unauthorized parties**

  Mitigation: Subcontractors are bound by the same confidentiality provisions as contractors to PPHS. All communications between CII Hub, EMR vendor data centres, Alberta Blue Cross and PPHS use secure, encrypted channels. The CII Hub is located in a secure data centre.

- **Risk 3**: **Loss of integrity of information**

  Mitigation: Use of a high availability data centre with tested backup and recovery processes and redundancy of systems minimizes this risk.

- **Risk 4**: **Loss, destruction or loss of use of information**

  Mitigation: Business continuity processes for the data centre meet PPHS requirements. Use of firewalls, intrusion detection and malware detection also help to minimize this risk.

- **Risk 5**: **Data centre located outside of Alberta**

  Mitigation: An information management agreement forms part of the contract with Orion Health and conforms to the Health Information Act and its regulations. The contract prescribes types and frequency of penetration testing and vulnerability assessments that must be completed. The results of this testing must be provided to PPHS.

CPAR

Access Controls

PPHS and its affiliates, including roster and registry administrators within ABC, will have access to patient attachment and affiliation information.

Registration and authentication procedures consistent with the Government of Alberta's Information and Security Standard are in place. User access requires verification of identity and credentials, and is tailored to the user's specific role. Primary providers and their affiliates must agree to terms and conditions before accessing CPAR.

Privacy Risks

- **Risk 1**: **Unauthorized use of information by internal or authorized parties**

  Mitigation: User access is monitored following the Alberta Provincial Logging and Audit Standards (PLAS). Alberta Blue Cross (ABC) and PPHS users must take mandatory privacy training. PPHS provides ongoing security and privacy training to affiliates.

  Government of Alberta employees sign a confidentiality agreement. Sanctions for breaches include fines, disciplinary action, and potential dismissal.

- **Risk 2**: **Unauthorized collection, use or disclosure of information by external parties**

  Mitigation: Information is stored in ABC's secure environment. There are security policies and standards in place covering the confidentiality of information and integrity of systems and data, including standards for data transmission, encryption and masking, and use of secure encrypted protocols.

- **Risk 3**: **Loss of integrity of information**

  Mitigation: Users are trained on proper data entry. Data exchanges between CII and CPAR are automated, with no end-user access. Validation process ensures rejection of corrupted or altered data.

- **Risk 4**: **Loss, destruction or loss of use of information**

  Mitigation: ABC corporate and departmental business continuity plans are in place, including an IT disaster recovery plan. A risk assessment framework will identify and prioritize assets, identify threats and potential impacts to loss. Panel submissions can also be re-created and re- processed if data is lost (via extraction from source EMR system).

eNotification of ADT Events

Privacy Risks

- **Risk 1**: **Loss, destruction or loss of use of information caused by changes made to the EMR system**

  Mitigation: Changes to the EMR vendor software are tested by PPHS to ensure there are no errors or defects introduced as a result of the changes.

- **Risk 2**: **Loss, destruction or loss of use of information caused by changes made to CII Hub**

  Mitigation: Changes to the CII Hub software are tested by PPHS to ensure there are no errors or defects introduced as a result of the changes.

- **Risk 3**: **Unauthorized collection, use or disclosure by unauthorized parties if new data flows are intercepted between data centres**

  Mitigation: All data transfers are secured through encryption protocols. Transmissions from the CII Hub to the Alberta Blue Cross (ABC) data centre for CPAR are also protected using a secure connection.

- **Risk 4**: **Disclosure of health information to the unauthorized party if ADT eNotifications are disclosed to the wrong provider by the EMR vendor**

  Mitigation: The submitting clinic ID and EMR product are captured by the CII Hub on inbound panel submissions, and then passed back to the EMR vendors as part of the ADT eNotifications. This provides an established linkage between patient, provider, clinic identification and EMR product that EMR vendors will use to determine the correct recipients for ADT eNotification delivery.

Section E – Policies and Procedures

PPHS' PIA details its organizational policies that facilitate compliance with the HIA. Participating custodians must also implement policies and procedures that facilitate HIA compliance within their practice. Custodians append their own policies to their CII PIA submission, as described above or could also refer to an existing PIA if they have submitted their policies and procedures as part of that submission in the last two years.

More Information

For further information about the CII project and Alberta Netcare, please visit the Alberta Netcare Learning Centre.