How does AHS meet its privacy obligations to patients while making information available through CCPP?

AHS has configured the Connect Care Provider Portal (CCPP) to allow authorized users to access the health information of AHS patient in Alberta. Access to health records requires a balance between making health information available when and where needed to support patient care and the need to protect the privacy, confidentiality, and security of health information.

Why is it necessary to monitor user access to the Connect Care Provider Portal?

Providers and their staff must only collect, use, and access health information required to support a health service.

CCPP user access is designed with safeguarding measures to protect health information. Monitoring user access ensures that end users are only accessing and using CCPP to support a health service for patients under their care.

Auditing users involves the systematic review of user access logs to ensure access is appropriate and is undertaken to support or provide a health service for the patient.

What is considered a privacy breach?

A privacy breach is any suspected or confirmed unauthorized access to information includes, but is not limited to attempting to gain access to health information not pertaining to a patient you are providing care for; gaining access in error to health information; accessing health information without a “need to know”; using another individual’s ID and password to gain unauthorized access; accessing your own information or the information of family, friends or relatives; sharing health information you acquired from CCPP with anyone who does not have a “need to know” the information, and adding or discovering inaccurate information associated with a patient record, for the purpose of completing job duties, individuals without a legal right of access i.e. the patient or their authorized representative and adding inaccurate information associated with a patient record. A privacy breach contravenes the CCPP Access Agreement and Alberta’s Health Information Act (HIA).

All instances of a suspected or confirmed privacy breach must be reported to privacy@ahs.ca and are subject to investigation pursuant to the organizations’ obligations under the HIA, and the signed CCPP Access Agreement.

What are the possible offenses and penalties under HIA legislation?

Persons that contravene the HIA by improperly accessing or using health information for purposes not related to their job or position, can be fined by the Office of the information and Privacy Commissioner of Alberta (OIPC) for an offense. Fines can be up to $200,000 individually, and up to $1,000,000 for the organization or the involvement of other persons as stated in the HIA.

Who is responsible for auditing the use of the CCPP?

Auditing is a shared responsibility between the owner of the CCPP, and the Lead Custodian(s) who authorize user access and use the CCPP in a health facility.

What are AHS’s Responsibilities Under the HIA?

The owner and operator of Connect Care is accountable under HIA for ensuring user access is monitored, in CCPP and that system audits are distributed and accessible to Lead Custodians. The organization is responsible for privacy breach investigations and mandatory breach reporting to the regulator.

What are the Clinic's Responsibilities?

The Lead Custodian on behalf of all Custodians at the clinic is accountable for complying with the HIA and the CCPP Access Agreement. This includes overseeing the clinics' user engagement and interaction with the information within the CCPP on a predetermined monthly schedule; reporting suspected or confirmed privacy breaches, participation in the investigation of privacy breaches as requested by AHS and fulfilling a formal notification/reporting requirement.

The Lead Custodian may delegate the implementation of their monitoring and auditing obligations to the Access Administrator for the clinic.

How is CCPP Audited?

System access and user activity in CCPP is electronically monitored, recorded and is auditable, which meets the compliance requirements for auditing under HIA.

Auditing reports identify which users accessed health information and will be used to aid in the investigation of suspected or confirmed privacy breaches by the required party(ies).

What audit reports are available in CCPP?

The Lead Custodian or Access Administrator may use the Managed Patient Access Summary report, the First Access Detailed report or the Unsuccessful First Access Attempts report for auditing purposes. These reports are intended to assist in the determination that access to information was consistent with the assigned role of the authorized staff member.

Managed Patient Access Summary report can be used to determine how often users at a site are accessing patient records. The report identifies two pieces of information, the total number of times patient records were accessed, and the number of unique patient records accessed.

First Access Detailed report can be used to identify users accessing patient records inappropriately by looking for a high number of First Access lookups and reviewing the reason for First Access. The report outlines the date/time a CCPP user is connected to a patient record and the reason selected for accessing the chart. Reasons include:

- Access Needed by Patient's PCP
- Emergency Care
- Referring Physician
- Hospital Care Team
- Other (please specify)

Unsuccessful First Access Attempts report displays potentially suspicious patterns of failed attempts users to gain access to patient records. The report can help to identify users who are "snooping" by repeatedly attempting to use First Access with small changes to the search data entered each time.

Where can I find the CCPP reports?

In the reporting activity click on My Reports.

Who has access to view the CCPP reports?

AHS, the Lead Custodian, and the Access Administrator (if applicable).

Who can I contact if I need assistance using the auditing reports in the CCPP?

For additional technical support, you can send a Customer Service Request message via the In Basket activity.

Does a Lead Custodian need to notify AHS if they become aware of a confirmed or suspected privacy breach, by either the Lead Custodian or other authorized staff at the clinic?

Yes, if a Lead Custodian becomes aware of a confirmed or suspected privacy breach involving any CCPP user, they must notify AHS within 24 hours of discovering the suspected or confirmed privacy breach. Both AHS and the Lead Custodian will work together to support any investigation, mandatory reporting, or notification requirements.

What are the key steps for responding to a suspected or confirmed privacy breach?

1. Respond
    a. Stop the unauthorized practice.
2. Report
    a. Notify AHS, send an email to privacy@ahs.ca
    b. AHS privacy will contact the Lead Custodian directly.
3. Investigate
    a. The investigation will be managed by AHS.
    b. All parties are responsible for contributing to investigation and resolution as directed by AHS.
    c. The AHS Health Information Continuity Team may be requested to participate as a liaison between AHS and the Lead Custodian.
4. Notification
    a. As the owner and operator of Connect Care, AHS will determine when to notify the OIPC and/or Alberta Health and identify activities required to meet mandatory breach reporting requirements, including notifications to affected individuals.
    b. The Lead Custodian on behalf of the clinic but depending on the circumstances of the breach and may be involved in the notification process.
5. Follow-up & Prevention
    a. Responsibility of the Lead Custodian

What are the consequences for not reporting a privacy breach or acting in contravention of HIA?

Conducting activity in contravention of HIA, can result in fines and possible prosecution. Adhering to mandatory breach requirements is important. If AHS is not satisfied that steps to investigate a suspected privacy breach are undertaken or appropriate action is not taken to report or remedy a privacy breach, access to the CCPP may be terminated or suspended for the entire clinic, and not just the user in question.