1 Introduction

AHS has prepared this summary for Connect Care Provider Portal (CCPP) users as a quick reference to help them understand their related responsibilities and outline the CCPP's privacy features, privacy risks and mitigations. This summary is based on extracts from the Connect Care Privacy Impact Assessment (PIA), which has also been provided to CCPP users. CCPP users are advised to refer to the full Connect Care PIA document for further details.

CCPP must users ensure that they understand the privacy risks and obligations to which they are subject, as set out in this PIA summary.

2 Connect Care Summary

Connect Care will transform how patient care is delivered and experienced in Alberta, providing the tools required to fully integrate standards driven healthcare services. It will be the bridge between information, healthcare teams and patients.

The foundation of Connect Care is a clinical information system (CIS) which, when fully implemented, will contain an integrated health record for every Albertan that will be available, as required and permitted, to support the delivery of health services across the province. Health information in Connect Care will also be used to support health system improvement activities including clinical improvement, program evaluation and policy development, health services provider education and clinical research.

Patients will be able to electronically access their health records and securely communicate with their health services providers, increasing their ability to be active participants in their health care. Finally, patients will benefit from the ability of their community-based care teams (i.e. family doctors) to review detailed records related to services provided by AHS and securely seek clarification when required.

3 Provider Portal Summary

The CCPP provides CIS access to community providers who are providing health services to AHS patients to improve the continuity of care for patients as they move throughout the health care system. CCPP gives secure, web-based access to patient information, order entry and referral management functions (incoming and outgoing), including support for messaging, information and file exchange, integrated care planning and many other care coordination activities.

Alberta Health Services
Connect Care

CCPP users can:

- View upcoming patient appointments with AHS specialists
- View test results in real-time
- View notes e.g., discharge summaries from inpatient admission or emergency department visits.
- Place and track the progress of referrals
- Receive notification of emergency department visits, inpatient admissions and discharges
- Communicate with AHS providers by sending them an In Basket message (e.g. where a CCPP user has a question about the medications listed on a discharge summary)
- Add a note to the patient chart. The note will be labelled as a Community Care Management encounter. This is visible in Chart Review for all Connect Care users and becomes part of the legal record of care.

In comparison to direct access to Connect Care, the CCPP has fewer interactive features. The provider role for the CCPP has limited functionality that allows CCPP users to impact the legal record of care. By default, providers are presented only with patients with whom they have a care relationship, as indicated in AHS records. Providers may access other patients' records after following a break-the-glass protocol where they enter a reason to access the record (e.g. providing care to a new patient). These accesses and requests to record new care relationships with patients are subject to AHS review.

4 PROVIDER PORTAL ONBOARDING

All CCPP users will need to complete the privacy training program described below for affiliate Hyperspace users. In addition to these requirements, CCPP users will need to complete the following steps to gain access:

1. During the Study period, AHS will deploy the CCPP to sites where the custodians met the "authorized custodian" requirements set out in the Alberta Electronic Health Record (EHR - Netcare) provisions of the HIA and the Alberta EHR Regulation within the last 2 years. For further Waves, AHS may revisit its approach to qualifications for eligibility to participate in CCPP.

2. Custodians must agree to the AHS Connect Care Provider Portal Access Agreement (Portal Access Agreement): Under this agreement, custodians agree to use the CCPP solely to provide health services to their patients who are also AHS patients. Custodians must agree to meet AHS privacy and security requirements and comply with AHS policies and procedures, including those related to access to and the correction of health information, patient expressed wishes, audit, incident management and investigation. Custodians will assume the role of "authorized approvers" at their site and in this capacity, may authorize their staff (i.e. their affiliates under HIA) to use the CCPP in accordance with AHS user provisioning requirements. A copy of the Portal Access Agreement is provided in Appendix #1.

3. All CCPP users must agree to the Connect Care Provider Portal User Terms & Conditions (User Terms): This is an online agreement. The User Terms require all users to use the CCPP solely to provide health services and to use health information in a limited manner, among other obligations. CCPP users must acknowledge that AHS may audit their use of the CCPP. The User Terms are attached as Appendix #2.

4. Complete AHS' Privacy and Security Self-Assessment and Certification (Self-Assessment): Custodians must certify they will:

   - comply AHS principles regarding health information privacy and safeguards,
   - prohibit snooping and account sharing by their staff,
   - conduct regular reviews of their security controls, and
   - comply with AHS requirements regarding incident response.

   The Self-Assessment is reviewed by AHS security personnel. Custodians must meet AHS requirements before they are granted CCPP access. A copy of the Self-Assessment (which sets out assessment criteria) is included in Appendix #3.

5. Complete the Expedited PIA process for CCPP: This process requires custodians who will be acting as "Authorized Approvers" under the Portal Access Agreement to send a PIA endorsement letter to the OIPC stating they understand their responsibilities under the Connect Care PIA and the Portal Access Agreement and that they have completed the Self-Assessment and Certification. A copy of the Expedited PIA cover letter is attached as Appendix #4.

5 Privacy and Security Features

Two-Factor Authentication
CCPP users will be accessing Connect Care from outside the AHS IT infrastructure and must use two-factor authentication in addition to logging in with a username and password combination. CCPP users will be issued a RSA hard token fob or mobile device soft token.

Encryption
CCPP is accessed via an internet browser. All information transmitted between providers and AHS via CCPP is protected with industry-standard encryption protocols. No CCPP data is stored on the community provider's computers.

User Activation and Deactivation

CCPP user activation and deactivation requests are managed through the AHS Identity and Access Management (IAM) system.

Authorized Approvers will manage and deactivate CCPP users according to the terms of the AHS Connect Care Provider Portal Access Agreement.

Session timeouts and account inactivity termination

A CCPP session will timeout after 10 minutes of inactivity. After this timeout the user will be required to log back in.

After 180 days of inactivity CCPP accounts will be terminated. User accounts may be reinstated, but only after the user re-completes applicable on-boarding processes, including mandatory privacy and competency training.

CCPP privacy monitoring and audit

All CCPP use is logged and is subject to AHS's privacy and security auditing policies and meets the Provincial Logging and Auditing Standard. For more information, see AHS Policies & Bylaws. (https://www.albertahealthservices.ca/about/Page210.aspx)

CCPP passes audit credentials (Provider ID, Patient ULI & Location ID) bi-directionally between Connect Care and Alberta Netcare for integrated sessions.

Connect Care enhanced confidentiality features

All Connect Care enhanced confidentiality features, such as private encounters, sensitive notes and break-the-glass functionality, are equally implemented in the CCPP and are described briefly below:

- Expressed wish management in Connect Care provides patients with an additional layer of privacy controls, these include functionality to provide:
  - Visitor restrictions to prevent unwanted visits or phone calls to a patient during their stay.
  - Confidential address allows patients to specify an alternative address to his or her primary address to which reminders, results, and other correspondence, is to be sent.
  - Confidential guarantor allows a patient to request to have their billing statement sent somewhere other than their permanent address.
  - Release of information restrictions allows special disclosure considerations to be visible at appropriate places within a patient's record.
  - Private encounters protect patient names from being shown to wayfinding, and information desk staff.
  - Break-the-glass creates a soft wall around an encounter that requires a user to re-enter his/her credentials and justify access prior to gaining access to the encounter information.
  - Sensitive note allows a patient to request that a particular note be less accessible or hidden from ordinary view.
  - Identity theft to alert staff about possible identity theft and permit them to assess the accuracy of health information attributed to the patient.
- Consent management to facilitate standardized and efficient practices for documenting informed consent to treatment, consent to the collection, use, and disclosure of health information for clinical and administrative purposes. Connect Care enables an electronic process for collecting signatures. When required consent and other authorization forms may still be printed, signed and scanned into Connect Care.

6 Requests from patients: Access to Information, Corrections and Disclosure Limitation

Under the Portal Access Agreement providers and AHS are required to collaborate in responding to request from patients regarding access to health information, requests to correct health information and requests to limit disclosure to health information.

Access to Information
AHS is responsible for responding to patients or their legal representatives who make requests for access to their health information under Part 2, section 8 of the HIA. AHS has established the following procedure:

A party who receives a request of this nature shall promptly notify the other party of the request in accordance with the requirements and time-frames set out in the HIA or other applicable legislation using the processes and procedures set out in the AHS Policies. AHS will be the party responsible for responding to requests for access or corrections to the Provider Data in its possession

Patients can ask AHS for copies of their own health information by following the steps below.

Fill out the Health Information Access Request form. Be as exact as possible when filling out this form. This helps us complete your request faster and ensures you receive all the documents you need.

1. Instructions to complete the form can be found at How do I fill out the Health Information Access Request form? You can fill out the form online and print the form or you can print the form and fill it out it manually.
2. Attach a copy of the required identification (ID) to verify your identity. For acceptable forms of ID, click on How do I verify my identity? Copies of your ID will be destroyed in a confidential, secure manner once your request is processed. No record of the ID numbers is kept. We only make note of the type of ID you provide.
3. Mail, fax or drop off your completed and signed request form and copy of ID to the attention of Access & Disclosure, Health Information Management at a hospital or health care centre where you received treatment.
4. If you do not know the mailing address of the hospital or health care centre, site contact information can be found by viewing the following service listing: Health Information - Access and Disclosure.

If you are asking for health information on behalf of another person, follow the process below.

1. Fill out the Health Information Access Request form. Be as exact as possible when filling out this form. This helps us complete your request faster and ensures you receive all the documents you need.
2. Instructions to complete the form can be found at How do I fill out the Health Information Access Request form? You can fill out the form online and print the form or you can print the form and fill it out it manually.
3. Attach copies of identification (ID) to verify your identity. For acceptable forms of ID click on How do I verify my identity? Copies of your ID will be destroyed in a confidential, secure manner once

your request is processed. No record of the ID numbers is kept. We only make note of the type of ID you provide.

4. The person on whose behalf you are acting will be required to complete the Authorization of Health Information Act Representative form. Alternatively, you may attach the required supporting documentation as indicated on the Health Information Access Request form.
5. Mail, fax or drop off your completed and signed request form; copy of ID and any supporting documents (if applicable) that show you have the authority to act on behalf of the other person to the attention of Access and Disclosure, Health Information Management at a hospital or health care centre where the person was treated.
6. If you do not know the mailing address of the hospital or health care centre, site contact information can be found by viewing the following service listing: Health Information - Access and Disclosure.

Correction Requests

AHS is responsible for responding to patients or their legal representatives who make requests to correct or amend their health information under Part 2, section 13 of the HIA. AHS has established the following procedure:

A party who receives a request of this nature shall promptly notify the other party of the request in accordance with the requirements and time-frames set out in the HIA or other applicable legislation using the processes and procedures set out in the AHS Policies. AHS will be the party responsible for responding to requests for access or corrections to the Provider Data in its possession

If you believe there is a mistake, error, and/or omission of information in the health record, you may request correction or amendment. **In support of your request, you must provide adequate proof or evidence.** For example, reports of x-ray or laboratory tests or documents showing a medical diagnosis might be needed to prove a certain medical condition exists. In addition, please note you may only request correction or amendment within a health record. **We cannot remove a health record created by an AHS health care professional, such as your physician, nurse, etc.**

Step 1: Complete this form and provide supporting documentation. No initial fee required.
Step 2: Send your form and supporting documentation by mail, email, or fax.

Information & Privacy,
5th floor, North Tower, Seventh Street Plaza, 10030 – 107 Street
Edmonton, Alberta T5J 3E4
Email:
Fax: 1-780-735-1666

Disclosure Limitation Requests

To the extent possible, providers are responsible for responding to requests from patients or their legal representatives regarding disclosures of their health information (“expressed wish requests”) under section 58(2) of the HIA. AHS has established the following procedure:

A party who receives a request of this nature shall promptly notify the other party of the request in accordance with the requirements and time-frames set out in the HIA or other applicable legislation using the processes and procedures set out in the AHS Policies.

AHS and the Provider shall collaborate and coordinate on all such information requests, subject to the following (unless otherwise agreed by the parties in writing or specifically addressed in the AHS Policies):

(i) AHS will be the party responsible for responding to requests for access or corrections to the Provider Data in its possession; and

(ii) to the extent practicable under the circumstances and depending on the nature of the Provider Data, any expressed wish by an individual relating to the disclosure of such individual's Provider Data shall be addressed by the Provider as the party who initially collected such Provider Data. Responses to an individual's request for information or an expressed wish by either AHS or the Provider, as the case may be, shall be in accordance with the requirements and time-frames set out in the HIA or other applicable legislation and as set out in the AHS Policies.

(iii) Subject to the processes and procedures set out in the AHS Policies, AHS and the Provider will coordinate and agree on each party's responsibility for making the necessary changes, corrections or additions to the Provider Data as applicable under the circumstances.

7 Privacy and Security Incidents

Under the Portal Access Agreement providers and AHS are required to inform each other as soon as practicable if they become aware of any actual or suspected breach of privacy, security or integrity of information in the CCPP. Providers and AHS are also required to collaborate on investigating and remediating incidents. AHS has established the following procedure:

- Take immediate steps to prevent any further privacy breaches,
- Contact the Information and Privacy Office @ 1-877-476-9874 to report the privacy breach, including a complete list of:
  - the names of individuals whose information was breached and the type of personal information that was breached
  - document a list of all employees who were involved in the breach or were involved in containing the breach
  - document where or to whom the personal/health information was disclosed
- Attempt to recover the disclosed information by arranging to have it returned to AHS. If the information cannot be returned, then AHS/Provider will ensure the information has been destroyed and that no copies of the information were made,
- If the incident involves laptops, memory sticks, phones or other electronic devices, the Repository Owner or the Repository Owner's delegate shall contact AHS Information Technology to report the security incident to the AHS Service Desk @ 1-877-311-4300.

8 Training

Users must complete privacy training (via video) and the "Introduction to Connect Care Provider Portal" prior to gaining access to the CCPP. Completion is monitored by AHS.

The following training materials and videos will be available from the home screen of the CCPP and can be accessed by users at any time.

- 5 eLearning videos
  - ECL200 – Introduction to Connect Care Provider Portal
  - ECL205 - Finding Patients through Managed Access
  - ECL210 - Placing Orders
  - ECL220 - Using In Basket
  - ECL230 – Monitoring Your Patients Events
- Quick start guide: step-by-step instructions
- Frequently asked questions

9 Organizational Privacy Management

AHS has established a Connect Care governance structure to ensure identifiable health information is collected/used/disclosed in compliance with the Health Information Act (HIA). The CCPP Access Agreement outlines the requirements for community providers to abide by. These requirements must be met by the community providers to gain access.

In addition to following the requirements of the CCPP Access Agreement, providers using CCPP are responsible for implementing and maintaining their own organizational privacy management, policies and procedures as required by sections 62 and 63 of the HIA.

10 Connect Care Provider Portal Privacy Analysis

AHS makes the CCPP available to community providers for the purpose of providing health services including continuing treatment and care to AHS patients. This is a custodian-to-custodian disclosure under the authority of HIA section 35(1)(a) (for any or all of the purposes listed in HIA section 27(1)(a) including providing health services). When community providers access the CCPP, they are collecting health information from AHS under the authority of section 20(b) and 22(2)(g) of the HIA. The CIS Portal Access Agreement that AHS enters into with providers limits use of the CCPP to the provision of health services.

11 Privacy Risk Mitigation

In order to ensure the privacy of individuals steps have been taken to mitigate the risks associated with the use of CCPP. The main risks and mitigation strategies have been included below for your information.

Risk	**Mitigation Strategy**
AHS discloses more health information than is essential to meet the intended purpose via Connect Care Provider Portal.	• The CCPP user agreement stipulates that the CCPP may be used only to collect health information required to provide health services to the user's patients that are also AHS patients. • Each CCPP user is only given access to health information of patients identified as having a care relationship with the CCPP user. CCPP users who use break the glass functionality to access other patients' health information are subject to audit. • CCPP soft launch, limits the risk by initially limiting use of the CCPP to a small number of users and sites. Following the soft launch period, AHS will evaluate CCPP processes including HIA compliance controls.
AHS discloses health information without due consideration of the patient's expressed request to limit disclosure.	Information subject to enhanced confidentiality in Connect Care is not accessible through the CCPP.
Risk of scanned document being attached to the wrong patient record.	CCPP user submits a Customer Service Request to have the document removed via In Basket message to HIM. CCPP users cannot delete uploaded documents on their own.
Risk of scanned document having malware included in content.	• AHS anti-malware solution scans all documents uploaded to CCPP. AHS responds to all malware alerts and mitigates malware risk in CCPP, following its standard anti-malware procedures.
AHS can't enforce its policies and procedures on non-AHS users.	• Auditing is conducted on the usage of CCPP on a regular basis. AHS can terminate a CCPP user's access if facilities or users are not abiding by the terms of their agreements with AHS.

12 FURTHER INFORMATION

To obtain a full copy of the Connect Care PIA or for further information about the Connect Care PIA, please contact AHS Legal and Privacy on the contact details set out below:

If your patients have further questions or concerns about privacy, security, access to information, or correction requests in CCPP please refer them to the following FAQ site:
https://www.albertahealthservices.ca/info/Page16171.aspx

Or

AHS Legal and Privacy intake:

Toll-free Intake Line: 1-877-476-9874
Toll-free Fax Line: 1-877-573-5107
Email: privacy@ahs.ca

Alberta Health Services
Connect Care

Patients who wish to register a formal complaint about their privacy, access to information or correction requests may contact:

AHS Legal and Privacy intake:

Toll-free Intake Line: 1-877-476-9874
Toll-free Fax Line: 1-877-573-5107
Email: privacy@ahs.ca

Office of the Information and Privacy Commissioner (Edmonton)

#410, 9925 - 109 Street
Edmonton, Alberta
T5K 2J8

Phone: 780-422-6860
Toll Free: 1-888-878-4044
Fax: 780-422-5682

13 APPENDICES

- Connect Care Provider Portal Access Agreement (Appendix #1)
- Connect Care Provider Portal User Terms & Conditions (Appendix #2)
- AHS Provider Portal Privacy & Security Assessment (Appendix #3)
- Expedited PIA Cover Letter (Appendix #4)