

Appendix 1

Type of Information	Data Elements	Purpose for the collection, use or disclosure.	Source of Information
Demographics	Unique Lifetime Identifier (ULI) Personal Healthcare Number (PHN) Medical Record Number (MRN) Municipality Province Postal Code Date of Birth Date of Death Gender (sex) Name Street Address Contact Information (Telephone Number, email address) Height/Weight Education General Financial (Household Income sources / ranges, personal income sources) Marital Status Sexual Orientation Gender Identification	Patient identification and verification. Treatment and care.	Patient Netcare Connect Care
Clinical (Diagnostic, Treatment & Care)	Health Service Provider Identifier Health Service Provider Name Health Service Provider Practice Municipality Health Service Type Health Service Facility Medication Amount of Benefit Paid Diagnosis Service Event Order Intervention Admission and Discharge Dates Dietary Information Physical Activity Smoking/Alcohol Use Past Medical History Social History Surgical History Adverse reaction/allergy documentation	Service Provider identification and verification, Treatment and care.	Netcare Connect Care



ALBERTA
HEALTH

*Office of the Minister
MLA, Red Deer-North*

JAN 08 2025

AR 225842

Athana Mentzelopoulos, President and Chief Executive Officer
Alberta Health Services
Kerry Bales, Chief Executive Officer
Recovery Alberta
14 Floor North Tower, Seventh Street Plaza
10030 107 Street NW
Edmonton AB T5J 3E4

Sent via email: Athana.mentzelopoulos@ahs.ca; ahscorp@ahs.ca; ceo@recoveryalberta.ca

Dear Athana Mentzelopoulos and Kerry Bales:

Alberta Health has determined that it is in the public's best interest to enable community health providers, who are authorized to access Alberta Netcare, to access all identifying patient information that is available in Connect Care (the "Connect Care information") via Alberta Netcare. Alberta Netcare is the provincial Electronic Health Record (EHR), also known as the Alberta EHR. Therefore, pursuant to section 56.3(6) of the *Health Information Act*, I request that Alberta Health Services (AHS) and Recovery Alberta (RA): Mental Health and Addiction Services), as custodians of the Connect Care information, make the Connect Care information accessible to authorized custodians through Alberta Netcare.

To fulfill this request, pursuant to Directive D3-2024 (Health System Refocus–Information Management/Information Technology Directive) issued on June 6, 2024, and Ministerial Order 802/2024, dated August 28, 2024, AHS and RA shall cooperate with each other and Alberta Health as information manager of the Alberta EHR to:

- (a) Take any steps necessary to make the Connect Care information accessible to authorized custodians via Alberta Netcare through the Connect Care Provider Portal or, upon further written notice from the Department of Health, via Alberta Netcare through alternative means to be specified in the notice;
- (b) To make the Connect Care Information accessible to authorized custodians via Alberta Netcare as set out in (a) in accordance with timelines specified by the Department of Health; and
- (c) Participate in the submission of any privacy impact assessment(s) or related matters the Department of Health requires in conjunction with access to Alberta Netcare.

Should you wish to discuss this request further, please contact Leann Wagner, Senior Assistant Deputy Minister, at Leann.Wagner@gov.ab.ca.

Sincerely,

Athana Menzelopoulos and Kerry Bales
Page 2

A handwritten signature in black ink, appearing to read 'Adriana LaGrange', with a stylized flourish extending from the end.

Adriana LaGrange
Minister of Health

cc: Leann Wagner, Senior Assistant Deputy Minister, Alberta Health



ALBERTA

Health

*Office of the Minister
MLA, Red Deer - North*

M.O. 804/2025

WHEREAS pursuant to section 1.1(1) of Alberta's *Provincial Health Agencies Act* (the **Act**), the Minister of Health (**Minister**), as oversight Minister, is responsible for the strategic direction of the health care system in Alberta;

WHEREAS section 1.9(1) of the Act established the acute care, primary care, continuing care and mental health and addiction health services sectors;

WHEREAS pursuant to section 1(l)(iv) Act, the Minister of Mental Health and Addiction is the sector Minister responsible for the mental health and addiction health services sector, including its strategic direction;

WHEREAS pursuant to section 1.92(1) of the Act, the Minister of Mental Health and Addiction, as sector Minister, made Ministerial Order 703/2024, establishing a provincial health agency for the mental health and addiction health services sector with the name "Recovery Alberta: Mental Health and Addiction Services" (**RA**);

WHEREAS pursuant to section 1(l)(ii) of the Act, the Minister is the sector Minister (by virtue of being responsible for the *Alberta Health Act*) responsible for the primary care health services sector and, pursuant to section 1.2(1) of the Act, is responsible for its strategic direction;

WHEREAS pursuant to section 1.92(1) of the Act, the Minister, as sector Minister, made Ministerial Order 330/2024, establishing a provincial health agency for the primary care health services sector with the name "Primary Care Alberta" (**PCA**);

WHEREAS pursuant to section 5.02(1) of the Act, the Minister, as oversight Minister, made Ministerial Order 800/2024 ordering that the affairs of the regional health authority, Alberta Health Services (**RHA**), shall commence to be wound up;

WHEREAS under section 16(1)(b) of the Act, the Minister of Health, as oversight Minister, may, if the Minister considers that it is in the public interest to do so, do any other thing that the Minister considers necessary to promote and ensure the delivery of health services in Alberta;

WHEREAS the Minister, as oversight Minister, has made Ministerial Order 800/2024 pursuant to sections 5.02(1) and (2) of the Act, ordering that the affairs of the RHA shall commence to be wound up in accordance with Division 2 of Part 3 of the Act;

WHEREAS section 5.03 of the Act authorizes the Minister, as oversight Minister, for purposes of winding up the affairs of the RHA to make various types of transitional orders, including orders:

- a) transferring to a successor the custody and control of any records of the RHA;
- b) authorizing the collection, use and disclosure, by the RHA or a successor, of:
 - a. "personal information" as defined in the *Freedom of Information and Protection of Privacy Act* (**FOIP**) (**Personal Information**); or
 - b. "health information" as defined in the *Health Information Act* (**HIA**), including individually identifying health information within the meaning of the HIA (**Health Information**); and
- c) providing for any other matters the oversight Minister considers necessary;

WHEREAS under section 16(1)(b) of the Act, the Minister of Health, as oversight Minister, may, if the Minister considers that it is in the public interest to do so, do any other thing that the Minister considers necessary to promote and ensure the delivery of health services in Alberta;

WHEREAS a ministerial order issued under sections 5.03 or 16(1)(b) of the Act is an enactment for the purposes of the *HIA* and the *FOIP*;

WHEREAS RA, PCA and the RHA are public bodies pursuant to sections 1(g)(ii.2) and 1(g)(v) of the *FOIP* and custodians pursuant to section 1(1)(f)(iv) of the *HIA*;

WHEREAS the RHA collects, uses, and discloses Health Information and Personal Information, including via its numerous information management (IM) and information technology (IT) systems (IM/IT Systems), and, prior to September 1, 2024, was the sole custodian of the Health Information that is accessible via the IM/IT Systems;

WHEREAS Ministerial Order 802/2024 was enacted effective September 1, 2024 to, among other purposes, require RHA to transfer custody and control of RHA's records, including records accessible via the IM/IT Systems, to RA, so that custody and control is shared by RHA and RA;

WHEREAS, as a result of the establishment of PCA, it is necessary for the RHA and RA to similarly transfer custody and control of records to PCA as successor custodian so that custody and control of the records is shared among RHA, RA and PCA, and for PCA to be able to use the IM/IT Systems, including for purposes of collecting, using, and disclosing Health Information and Personal Information accessible via those systems, in order for each of RHA, RA and PCA to fulfil their respective legal responsibilities and exercise their respective authorities;

WHEREAS it is not technologically possible within certain of the RHA's current IM/IT Systems to segregate Health Information and/or Personal Information contributed to the IM/IT Systems by RHA, RA and PCA, such that it is not possible to limit the sharing of custody or control to discreet records among the RHA, RA and PCA;

WHEREAS it would be detrimental to segregate Health Information and/or Personal Information as among the RHA, RA and PCA as this would fail to support the delivery of quality health services to patients, irrespective of whether it was technologically possible to segregate such information;

WHEREAS as a result of this technological limitation, it is necessary for the RHA, RA and PCA to seamlessly share as amongst them on an ongoing basis all records accessible via certain of the IM/IT Systems in order for RHA, RA and PCA to fulfil their own legal responsibilities and exercise their respective authorities;

WHEREAS to ensure seamless transition from the RHA and RA to PCA as a successor, of responsibility for the delivery of health services and the oversight and coordination of the delivery of health services in the health services sector for which PCA was established and to the extent necessary for each of the RHA, RA and PCA to fulfil their own legal responsibilities and exercise their respective authorities, it is necessary:


- a) pursuant to sections 5.03(1)(e) and (l) of the Act, sections 33, 39, 40(1)(c), (e), (f), and 40 of the *FOIP*, and sections 20, 27, 35, 36 of the *HIA*, for the RHA and RA to transfer custody and control of records, including records accessible via the IM/IT Systems, to PCA, so that custody and control of the records is shared among RHA, RA and PCA;
- b) pursuant to sections 5.03(1)(l) of the Act and Directive D3-2024 (Health System Refocus-Information Management/Information Technology Directive, issued on June 6, 2024), for the RHA to make available the IM/IT Systems for use by PCA and for the RHA to be PCA's information manager pursuant to section 66(1) of the *HIA* (**Information Manager**), of the Health Information accessible via the IM/IT Systems;
- c) pursuant to sections 5.03(1)(i) and (l) and 16(1) of the Act, sections 20, 27, 35, and 36 of the *HIA*, and sections 33, 39, 40(1)(f) of the *FOIP*, for the RHA, RA and PCA to seamlessly share records on an ongoing basis with each other, including records accessible via the IM/IT Systems, to ensure there is no disruption to continuity of care, clinical operations, or the patient experience during the transition, and to promote the objectives of planning and resource allocation, health system management, public health surveillance, and health policy development in Alberta;

WHEREAS the Minister considers it is in the public interest to ensure that RHA, RA and PCA are authorized to share Health Information and Personal Information with each other, including via the IM/IT Systems, during the period of the winding up of the affairs of the RHA to ensure seamless delivery of health services in Alberta during the transition; and

THEREFORE, I, ADRIANA LAGRANGE, Minister of Health, as oversight Minister, pursuant to sections 5.03(1) and 16(1)(b) of the Act, do hereby order the following to be effective February 1, 2025:

1. To the extent necessary for each of the RHA, RA and PCA to fulfil their own legal responsibilities and exercise their respective authorities, RHA and RA to transfer custody and control of RHA's and RA's records, including records accessible via the IM/IT Systems, to PCA, so that custody and control is shared by RHA, RA and PCA,;
2. RHA to enable persons authorized by PCA, and to continue to enable persons authorized by the RHA and RA, to access and use the IM/IT Systems and to secure such additional rights as may be necessary from applicable third party licensors, so that each of the RHA, RA and PCA can fulfil their own legal obligations and exercise their respective authorities, including for the continued delivery of patient care, and for the RHA to act as PCA's Information Manager of the Health Information accessible via the IM/IT Systems;
3. To the extent necessary for the RHA, RA and PCA to fulfil their own legal responsibilities and exercise their respective authorities, RHA, RA and PCA to seamlessly share with each other the records referred to in section 1 of this Order on an ongoing basis to ensure there is no disruption to continuity of care, clinical operations, or the patient experience during the transition, and to promote the objectives of planning and resource allocation, health system management, public health surveillance, and health policy development in Alberta;
4. RHA, RA and PCA may access, collect, use and disclose Health Information and Personal Information in the manner described under sections 1, 2, and 3 of this Order, in order to fulfil their respective legal obligations and exercise their respective authorities; and
5. In the event of a conflict or inconsistency between this Order and either the HIA or the FOIP, this Order prevails.

DATED AT Red Deer, Alberta this 29th day of January, 2025.


ADRIANA LAGRANGE
MINISTER OF HEALTH

DRAFT

DATE

Information and Privacy Commissioner
Suite 410, 9925-109 Street NW
Edmonton, AB T5K 2J8

Dear Information and Privacy Commissioner:

**Re: Privacy Impact Assessment for Alberta Netcare Portal and Connect Care Provider Portal
[CUSTODIAN NAME]**

I am submitting this PIA for Alberta Netcare Portal (ANP), including access to Connect Care Provider Portal (CCPP) via ANP. I am making this submission under the expedited PIA process originally described in Alberta Health's PIA for ANP (OIPC file H3879).

Alberta Health has made the latest PIA for ANP available to me, as well as the amendment to the ANP PIA that describes CCPP access via ANP. Further, Alberta Health has provided a summary of Alberta Health Services' (AHS) Connect Care PIA for my review which includes relevant sections that describe CCPP (OIPC file 032045).

Commented [BH1]: Eventually, we'll have OIPC file numbers to refer to that should be inserted into this letter.

I understand my related responsibilities as a Netcare "authorized custodian," under Part 5.1 of the *Health Information Act* (HIA) and the *Alberta Electronic Health Record Regulation* and as described in Sections A, C and D of the latest ANP PIA Alberta Health submitted on my behalf.

In accordance with section 3 of the *Alberta Electronic Health Record Regulation* I have completed a Provincial Organizational Readiness Assessment (pORA) and submitted it to Alberta Health for approval and will agree to the Alberta Netcare Body of Rules (described in the latest ANP PIA).

I have also signed the AHS Connect Care Provider Portal Access Agreement ("the CCPP Access Agreement"). As such, AHS has reviewed and accepted my CCPP Privacy and Security Self-Assessment and Certification, which asserts that I have met AHS privacy and security requirements regarding CCPP use.

I understand that this PIA applies to my use of ANP and my use of CCPP via ANP only and that I am responsible for maintaining and updating my HIA policies. Further, I understand that I am responsible for submitting PIAs to you for review and comment for any other proposed systems under my custody or control that collect, use and disclose identifying health information, as required by section 64 of the HIA.

[OPTION 1]

Please find attached a copy of my policies, as required by section 63 of the *Health Information Act* (HIA) and in support of Sections B and E of the OIPC PIA Requirements.

[CUSTODIANS REVIEW AND ADAPT WHERE NECESSARY MODEL POLICIES PROVIDED BY THEIR HEALTH PROFESSIONAL COLLEGE/ASSOCIATION]

[OPTION 2]

DRAFT

I have previously submitted a PIA to you for my [PRACTICE MANAGEMENT SYSTEM NAME] system, which was accepted on [DATE] file number [OIPC file #]. I have reviewed the policies I included with that submission and, in my opinion, they are sufficient to cover my use of ANP [OR] I have made the attached policy changes to accommodate my use of ANP. Please consider these policies in support of Sections B and E of the PIA Requirements.

Yours truly,

CUSTODIAN NAME

AHS CONNECT CARE PROVIDER PORTAL ACCESS AGREEMENT

BETWEEN:

ALBERTA HEALTH SERVICES
(“AHS”)

- and -

THE PROVIDER
(the Custodian named on the signature page of this Agreement)

RECITALS:

- A. AHS has implemented a provincial clinical information system, associated databases, third party applications and related health care initiatives branded as "Connect Care" which includes an external-facing portal called the Connect Care Provider Portal (the “CCPP”).
- B. The Provider provides Health Services to patients who are also patients of AHS and now wishes to use the CCPP to support the provision of those Health Services as well as obtain access for the Provider’s Authorized Staff.
- C. The Provider has demonstrated that it meets AHS’ prerequisites for use of the CCPP and AHS has agreed to permit the Provider to use the CCPP subject to the terms and conditions of this Agreement.

NOW THEREFORE for good and valuable consideration, the adequacy of which is hereby acknowledged, the parties hereby agree on the terms and subject to the conditions set forth in this Agreement as follows:

1.0 DEFINITIONS

- 1.1 Unless otherwise defined in the recitals or body of this Agreement, capitalized words have the following meanings:
 - (a) “**Access Administrator**” means one of the Provider’s Personnel authorized in accordance with the AHS Policies to manage access to the CCPP at the Clinic. An Access Administrator does not have to be a user of the CCPP and does not have to be a Custodian.
 - (b) “**Agreement**” means this AHS Connect Care Provider Portal Access Agreement. The Provider needs to execute a separate Agreement for each Clinic where the Provider delivers Health Services.
 - (c) “**AHS Policies**” means all rules, regulations, processes, procedures, directives, policies and bylaws in force and applicable to the CCPP published on AHS’ external website or in the CCPP or otherwise provided to the Provider by AHS, including as set out in user guidelines and frequently asked questions, all as may be amended by AHS from time to time.
 - (d) “**Authorized Staff**” means a subset of the Personnel authorized to use the CCPP.
 - (e) “**Claims**” means any and all claims, demands, complaints, actions, suits, causes of action, orders, charges or other similar processes, assessments or reassessments, judgments, debts, liabilities, expenses, fines, penalties, costs, damages, settlements or losses of any kind and all costs incurred in investigating or pursuing any of the foregoing or any proceeding relating to any of the foregoing.

- (f) “**Clinic**” means the location, environment or other work arrangement (i.e. remote service delivery model) in which the Provider and the Authorized Staff provide health services.
- (g) “**Confidentiality and User Agreement**” means AHS’ standard form confidentiality and user access agreement appearing at the end of AHS’ mandatory online privacy training.
- (h) “**Connect Care**” means AHS’ provincial clinical information system, databases and integrated third party applications.
- (i) “**Custodian**” means a custodian as defined in the HIA.
- (j) “**Effective Date**” means the date the Provider signs this Agreement.
- (k) “**End User Terms**” means the online End User Connect Care Provider Portal End User Terms & Conditions, as amended from time to time.
- (l) “**Epic**” means Epic Systems Corporation, the software vendor for the CCPP.
- (m) “**Epic Addendum**” means the acknowledgement by the Provider of Epic’s confidential and proprietary rights in the CCPP which is attached as Schedule A to this Agreement.
- (n) “**Epic Agreement**” means the Master License, Support and Services Agreement between AHS and Epic.
- (o) “**FOIPP**” means the *Freedom of Information and Protection of Privacy Act* (Alberta).
- (p) “**HIA**” means the *Health Information Act* (Alberta) and any regulations made thereunder.
- (q) “**Health Information**” means health information as defined in the HIA.
- (r) “**Health Services**” means health services as defined in the HIA.
- (s) “**Lead Custodian**” means the Custodian identified in Schedule B as the responsible Custodian at the Clinic. The Lead Custodian may be the Provider and does not need to be a user of the CCPP.
- (t) “**Personal Information**” means personal information as defined in FOIPP.
- (u) “**Personnel**” means any and all of the individuals employed or contracted by the Clinic.
- (v) “**PIA**” means Privacy Impact Assessment.
- (w) “**Privacy Laws**” means the HIA, FOIPP, the *Personal Information Protection Act* (Alberta), and the *Personal Information Protection and Electrical Documents Act* (Canada) as such acts may be modified or replaced from time to time.
- (x) “**Provider**” means the individual Custodian who executes this Agreement.
- (y) “**Provider Data**” means information entered by the Provider or the Authorized Staff into the CCPP.
- (z) “**Research**” means those research activities undertaken pursuant to Section 27(1)(d) or Section 27(2) of the HIA by persons properly authorized in compliance with the HIA.

- (aa) **“Self-Assessment”** means the Privacy & Security Self-Assessment that must be completed by the Lead Custodian certifying that the Clinic meets or exceeds AHS’ requirements for the CCPP.
- (bb) **“Schedule A”** means Schedule A attached and incorporated into this Agreement.
- (cc) **“Schedule B”** means Schedule B attached and incorporated into this Agreement.

2.0 CISA PRINCIPLES AND DISPUTE RESOLUTION

- 2.1 AHS collaborated with the Alberta Medical Association (“AMA”) and other key stakeholder groups in the provincial health care system to develop the “Clinical Information Sharing Approach for the AHS Clinical Information Systems” (“CISA”). AHS and the Provider agree to adopt the principles set out in the CISA, adjusted as appropriate to the CCPP, to inform and guide their activities under this Agreement.
- 2.2 The AMA has also reviewed and collaborated with AHS to develop the terms and conditions of this Agreement, the Self-Assessment and other documentation and guides for the CCPP.
- 2.3 AHS and the Provider agree to refer any matters arising in relation to this Agreement to the Information Stewardship Committee established under the CISA for dispute resolution purposes.

3.0 AHS REQUIREMENTS

- 3.1. AHS agrees to permit the Provider and the Authorized Users to access and use the CCPP for the provision of Health Services, subject always to the following AHS requirements and conditions:
 - (a) The Provider must sign the Epic Addendum.
 - (b) The Provider must designate a Lead Custodian and an alternate Lead Custodian (if possible) on Schedule B. The Lead Custodian is responsible for carrying out the Provider’s obligations under this Agreement.
 - (c) The Provider will ensure that the Lead Custodian completes the Self-Assessment and any additional Self-Assessments AHS requires from time to time.
 - (d) The Provider agrees and acknowledges that AHS has the right at any time and upon reasonable notice by AHS, to inspect and audit the Clinic’s systems, equipment and facilities to ensure continued compliance with the Self-Assessment and this Agreement.
 - (e) The Provider will identify the list of Authorized Staff on Schedule B and must ensure that this list is updated with all changes in accordance with the AHS Policies.
 - (f) The Provider, or the Lead Custodian, has the option to designate an Access Administrator to be responsible for ensuring changes to the Authorized Staff are managed in a timely fashion.
 - (g) The Authorized Staff will be limited to only those Personnel who need to use the CCPP in connection with the provision of the Health Services on behalf of the Provider.
 - (h) The Provider and each of the Authorized Staff must complete AHS’ mandatory privacy training and execute the Confidentiality and User Agreement at the end of the course.
 - (i) The Provider and each of the Authorized Staff must take the applicable competency training for use of the CCPP, as prescribed by AHS from time to time.

- (j) The Provider agrees to cooperate, and will cause the Authorized Staff to cooperate with any auditing or monitoring program required by the AHS Policies and is aware and acknowledges that:
 - (i) an audit log will be maintained that demonstrates all access events made to the CCPP;
 - (ii) access events will be proactively monitored by AHS and in response to complaints and/or breach investigations; and
 - (iii) inappropriate access events will be subject to consequences which may include suspension of access to the CCPP and/or termination of this Agreement.
- (k) The Provider will not allow any person to access the CCPP other than the Authorized Staff.
- (l) The Provider is responsible for:
 - (i) ensuring the Authorized Staff comply with this Agreement and the Privacy Laws;
 - (ii) obtaining separate user identification for each Staff Member, understanding that "shared" or "reused" user privileges are not permitted;
 - (iii) notifying or having the Access Administrator notify AHS immediately in writing when user access privileges are to be suspended or revoked or when any Authorized Staff no longer require access to the CCPP such as when the user changes roles or no longer works at the Clinic. The Provider shall comply with all of AHS' instructions regarding deactivation of any Authorized Staff' accounts;
 - (iv) ensuring Authorized Staff keep log-in information confidential, do not use any third party log-in information (whether that of any Personnel or any of AHS' personnel, employees or contractors), notifying and informing AHS' local Information Technology (IT) Service Desk of any changes to such individual's log-in information and not leaving workstations unattended such that the CCPP may be viewed by any third party; and
 - (v) ensuring Authorized Staff do not use the CCPP other than strictly for the purposes for which it is intended and required to be used and that they enter complete and accurate data and information into the CCPP, as applicable.
- (m) The Provider will comply, and will cause the Authorized Staff to comply with the rules and applicable procedures governing collection, access, use and disclosure of Health Information and Personal Information for use of the CCPP set out in the AHS Policies and the Privacy Laws.
- (n) The Provider will ensure the Clinic has filed an up-to-date organizational PIA with the OIPC.
- (o) As required by Section 58(1) of the HIA and the "least amount" principle described in that provision, the Provider and the Authorized Staff must only collect, use, access and disclose Health Information and Personal Information within the CCPP as strictly necessary to provide Health Services for an individual patient and will ensure that they do not collect, use, access and disclose the Health Information and Personal Information of other patients which is available in the CCPP.
- (p) The Provider will use reasonable efforts to ensure that no person or entity gains unauthorised access to, or use of, the CCPP. The Provider shall implement reasonable security measures and controls as necessary to provide such security safeguards on an administrative, technical and physical level

that protect the confidentiality of Health Information and Personal Information.

- 3.2. The Provider acknowledges that AHS must support a common provincial health care system rather than the specific needs of a single organization or individual. Accordingly, AHS will use commercially reasonable efforts to provide the CCPP using the same level of service that AHS provides to AHS end users.

4.0 PRIVACY AND DATA PROTECTION

- 4.1. The parties shall each comply with the applicable Privacy Laws in respect of the collection, use, access and disclosure of Health Information and Personal Information under this Agreement.
- 4.2. Each of the parties represents, warrants and covenants to the other that it has taken reasonable steps in accordance with Section 60 of the HIA and Section 8 of the HIA regulations to maintain administrative, technical and physical safeguards as applicable to their respective roles in respect of the CCPP in order to meet the requirements set forth in such provisions of the HIA. AHS and the Provider will comply, and in the case of the Provider it will ensure that its Authorized Staff comply, with the Privacy Laws. In the case of the Provider, such safeguards shall be no less rigorous than such safeguards implemented for its own operations, which in no event shall be less than safeguards which meet a reasonable standard of care.
- 4.3. The parties will amend this Agreement as may be necessary for continued compliance with Privacy Laws or as may be reasonably recommended from time to time by the OIPC and will at all times cooperate in good faith to protect the confidentiality and security of the Health Information and Personal Information.
- 4.4. AHS and the Provider agree that Health Information is individually identifying diagnostic, treatment and care information which is being disclosed to each other under the authority of Section 35(1)(a) of the HIA and is being collected by each party pursuant to Section 22(2)(g) and similar sections in applicable Privacy Laws for the purpose of providing Health Services to individual patients as required on a case by case basis. Despite the foregoing going, the CCPP shall not be used by the Provider, or any of its Authorized Staff, for Research. To the extent that AHS may make the CCPP available to the Provider or any of the Authorized Staff for Research in the future, additional agreements are required.
- 4.5. AHS agrees to provide the Provider with reasonable access to any Provider Data which the Provider enters into the CCPP. Such access will be in accordance with the AHS Policies. Access will not be denied by AHS except when access is unavailable due to technical difficulties, circumstances beyond AHS' reasonable control, or is restricted due to agreed reasonable security or privacy requirements.
- 4.6. AHS agrees to amend any Provider Data upon Provider's request in accordance with the Privacy Laws and the processes and procedures set out in the AHS Policies subject to the technical capabilities of the CCPP.
- 4.7. The parties agree to notify each other in accordance with the AHS Policies if either becomes aware of an actual or suspected breach of the privacy, security or integrity of Health Information or Personal Information in the CCPP. Each party shall take actions necessary to mitigate harm resulting from such a breach as required by applicable Privacy Laws and cooperate as necessary and in accordance with the AHS Policies to investigate the breach and confirm their respective reporting obligations to the OIPC. The Provider will also cooperate and implement reasonable recommendations made by AHS with respect to use by the Provider and the Authorized Staff of the CCPP.
- 4.8. Individual patients may have the right to request access or corrections to the Provider Data or make an expressed wish relating to the disclosure of the individual's health information under the HIA or other legislation. 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) due to the nature of the functionality of the CCPP, 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. 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 set out in the AHS Policies.

- 4.9. The parties shall collaborate as necessary so that patients are properly informed of the potential uses and disclosures of their Health Information and Personal Information within the CCPP. Such notice shall describe the uses and disclosures of the Provider Data to AHS and provide contact information for patients in the event they have any questions. AHS shall post its standard notice in its facilities and provide contact information for its Information & Privacy Office and the parties agree that this notice meets AHS' obligation under this section.

5.0 TERM, TERMINATION AND DISPUTE RESOLUTION

- 5.1. The term of this Agreement shall commence on the Effective Date and shall continue until terminated by the parties in accordance with this Article 5.
- 5.2. The Provider may terminate this Agreement for any reason on thirty (30) days' prior written notice to AHS.
- 5.3. Subject to Section 5.6, AHS may terminate this Agreement immediately upon notice for any breach by the Provider or its Personnel of any of the Provider's obligations under this Agreement, including without limitation any breach of the Privacy Laws.
- 5.4. AHS reserves the right to terminate an individual Staff Member's access to the CCPP in accordance with AHS then current policies and procedures if the Staff Member has not accessed the CCPP for a period in excess of 180 days. Any reinstatement of an individual's access to the CCPP will be managed in accordance with the AHS Policies.
- 5.5. AHS may also terminate this Agreement, in whole or in part, in the event AHS determines, in its sole discretion, to discontinue making the CCPP generally available to users by providing the Provider with reasonable written notice consistent with the timing and manner that AHS provides to the rest of the users of the CCPP.
- 5.6. The Provider reserves the right to refer any termination of this Agreement by AHS pursuant to Section 5.3 to the CISA Information Stewardship Committee for dispute resolution purposes.
- 5.7. The provisions of this Agreement which by their nature and intent are intended to survive termination, including but not limited to Article 7 (Confidentiality) shall survive to the extent necessary to give them full effect, including those provisions and obligations pertaining to Health Information and Personal Information.

6.0 AUTHORITY OF THE LEAD CUSTODIAN

- 6.1. By executing this Agreement, the Provider hereby agrees and confirms that the Lead Custodian identified in Schedule B shall represent the Provider with respect to the subject matter of this Agreement and hereby authorizes the Lead Custodian to execute the Self-Assessment and any additional agreement, instrument or documentation as may be required by AHS from time to time in relation to this Agreement on behalf of the Provider.

7.0 CONFIDENTIALITY

- 7.1. For the purposes of this Article 7:

“Confidential Information” of a party means any of the party’s confidential or proprietary information or material that is not public which may be acquired by, or become available to, the other party as a result of the matters referred to in this Agreement or out of the performance of obligations or taking of actions contemplated by this Agreement and includes, without limitation:

- (a) information contained in the data management systems of the party;
- (b) financial, operational, personal or business information, records and plans of or relating to the party or third parties, including without limitation, Epic;
- (c) Health Information and Personal Information;
- (d) any information which is required to be kept confidential by statutory or regulatory requirements as same may be amended, revised or substituted from time to time;
- (e) any information that the disclosing party advises the receiving party in writing is confidential or is marked or labelled confidential; and
- (f) any other information which by its nature is to be kept confidential.

- 7.2. Each party acknowledges that in it may come into possession of Confidential Information of the other party and therefore agrees to:

- (a) hold, and shall cause its affiliates, directors, officers, members, employees, advisors and authorized agents or representatives to hold, all Confidential Information of the other party in strict confidence and shall ensure the Authorized Users are bound by written obligations to protect the Confidential Information;
- (b) not collect, access, use, publish, distribute or disclose the other party’s Confidential Information except as necessary to perform its obligations hereunder; and
- (c) use all reasonable efforts to protect the other party’s Confidential Information against unauthorized access, use or disclosure.

- 7.3. Except for any Health Information or Personal Information, the foregoing obligations of confidentiality shall not apply to Confidential Information that the receiving party can demonstrate:

- (a) was known to the general public prior to its receipt from the other party or subsequently becomes known to the public through no fault of or action by the receiving party; or

- (b) is independently derived or developed without benefit of any of the disclosing party's Confidential Information.

Confidential Information may be disclosed by a receiving party to the extent required by applicable law, provided that the disclosing party is given reasonable notice and opportunity to seek to prevent or limit its disclosure.

- 7.4. The parties acknowledge that its failure to comply with the provisions of this Article 7 may cause irreparable harm to a disclosing party entitling such disclosing party to seek immediate injunctive relief, in addition to any other remedies to which it may be entitled.

8.0 DISCLAIMER; LIABILITY AND INDEMNITY

- 8.1. Unless expressly provided in this Agreement, the CCPP is provided "as is" without any representations, warranties or conditions of any kind. AHS specifically disclaims any and all liability in relation to, or resulting from the Provider's and its Authorized Staff's use of the CCPP. Use of the CCPP shall be at the Provider's own discretion and risk.
- 8.2. To the maximum extent permitted by applicable law, AHS disclaims all representations, warranties and conditions, express or implied, including the implied warranties of non-infringement, merchantability, and fitness for a particular purpose. AHS further disclaims any representation, warranty or condition that the CCPP Service will meet the Provider's requirements or will be constantly available, uninterrupted, timely, secure, or error-free.
- 8.3. Except for the indemnity provided by AHS set out in Section 8.5, the Provider's sole and exclusive remedy against AHS and its Affiliates, officers, directors, members, employees, contractors, consultants, agents, and licensors or their respective successors in relation to the CCPP is to stop using the CCPP.
- 8.4. Subject to Section 8.5, in no event shall either party be liable to the other party for any special, indirect, incidental, consequential or punitive damages or for damages to personal property or any loss or damages relating to medical injury, personal injury, death, improper diagnosis, care or treatment, inaccurate information, or any other Claims that are connected with the other party's use of, misuse of, or inability to use the CCPP, regardless of the cause or cause of action. The limitations under this Section will apply even if they knew of or could have anticipated that such damages were possible.
- 8.5. The Provider and AHS (each an "**Indemnifying Party**") will be liable to and indemnify, defend, and save the other party (each an "**Indemnified Party**") harmless from any and all third party Claims which the Indemnified Party may incur, suffer or be required to pay arising out of or in any way related to the Indemnifying Party's breach of this Agreement, the Privacy Laws or the Indemnifying Party's negligence or wilful misconduct in connection with the CCPP, including without limitation, a third party Claim for death, bodily injury or damage to real, tangible or intangible property, except to the extent such third party Claim arises out of the negligence or wilful misconduct of the Indemnified Party. For clarity, the mutual indemnification obligations of the parties set out in this section will apply to any liability, loss, damages, costs, expenses and settlement amounts arising out of a decision or order by the OIPC arising from the activities of AHS, the Provider or the Authorized Staff including the cost of responding to any complaint of an unauthorized disclosure of Health Information or Personal Information.

9.0 ASSIGNMENT

- 9.1. AHS may freely assign this Agreement or any of its rights and obligations hereunder (without the requirement to give notice to, or obtain consent from, the Provider).

- 9.2. The Provider shall not be entitled to assign this Agreement or any of their respective rights or obligations hereunder to any person without AHS' prior written consent, such consent not to be unreasonably withheld.

10.0 GENERAL

- 10.1. Every request, notice, delivery or written communication provided for or permitted by this Agreement shall be in writing and delivered to, or mailed, postage prepaid, or faxed to the parties as set out below:
- (a) If to Provider, the Provider's address provided on Schedule B; and
 - (b) If to AHS:

Alberta Health Services
Information and Privacy Office
10101 Southport Road S.W.
Calgary, AB T2W 3N2
Fax: 403 943-0429
- 10.2. The parties agree that the provisions of this Agreement requiring performance or fulfillment after the expiration or early termination of this Agreement, including Articles 7, 8, 9 and such other provisions as are necessary for the interpretation thereof, the nature and intent of which is to survive termination or expiration of this Agreement, shall survive the expiration or earlier termination of this Agreement.
- 10.3. This Agreement shall not be modified, amended, or in any way varied or changed, except by a duly written executed instrument by the parties.
- 10.4. This Agreement shall be governed by and construed pursuant to the laws in force in the Province of Alberta.
- 10.5. Each provision of this Agreement shall be severable from every other provision of this Agreement for the purpose of determining the legal enforceability of any specific provision unless to do so affects the entire intent and purpose of this Agreement.
- 10.6. Each party shall, with reasonable diligence, do all such things, provide all such reasonable assurances and execute and deliver such further documents or instruments as may be required by the other party in order to give effect to and carry out the provisions of this Agreement.
- 10.7. This Agreement and the End User Terms set out the complete understanding of the parties with respect to this subject matter and supersede all other prior and contemporaneous agreements, written or oral, between them. To the extent of any conflict or inconsistency between the End User Terms and any term of this Agreement, the terms of this Agreement shall prevail to the extent of the conflict or inconsistency.
- 10.8. This Agreement is the written memorandum and documentation of an agreement entered into between the parties on and as of the Effective Date.
- 10.9. This Agreement may be executed in any number of counterparts, each of which will be deemed to be an original, and all of which taken together will be deemed to constitute one and the same instrument. Delivery of an executed signature page to this Agreement by a party by electronic transmission will be as effective as delivery of a manually executed copy thereof by such party.

IN WITNESS WHEREOF each party has signed this Agreement with effect upon the Effective Date.

ALBERTA HEALTH SERVICES

By: _____
Name:
Title:
Date:

By: _____
Name:
Title:
Date:

Name of Individual Custodian (Print Above)

Signature

Effective Date

Schedule A
Epic Affiliate Addendum

THIS AFFILIATE ADDENDUM to the Master License, Support and Services Agreement between Epic Systems Corporation (“Epic”) and Alberta Health Services (“AHS”) made effective October 13, 2017 (the “Agreement”) is made effective on the date written below (the “Effective Date”).

RECITALS:

- A. Epic and AHS entered into the Agreement;
- B. The undersigned physician, corporation, professional corporation, partnership or other legal person is an “Affiliate” for the purposes of the Agreement; and
- C. The Affiliate wishes to use the Program Property and understands and acknowledges that it must execute and deliver to AHS this acknowledgement (“Acknowledgement”).

By executing this Acknowledgement, and in consideration of being granted the right to use the Program Property by AHS and Epic, the Affiliate hereby acknowledges, covenants, agrees and represents the following:

- 1. This Acknowledgement is an Affiliate Addendum referred to in Section 14(a)(iv) of the Agreement.
- 2. The Affiliate agrees to adopt, be bound by, observe and perform the terms and conditions of the Agreement as if the Affiliate were AHS (referred to as “You” in the Agreement) under the Agreement, and accordingly agrees that Epic is an intended third party beneficiary of this Acknowledgement.
- 3. The Affiliate agrees that Epic is entitled to enforce directly against the Affiliate all of the terms and conditions of the Agreement, including any exclusion and limit on the liability of Epic to AHS in the Agreement, as if the Affiliate had been originally named as an additional party to the Agreement.
- 4. Despite Section 2 of this Acknowledgement, Sections 13 (Your Right to Transfer This Agreement), 14 (Use of Program Property by Affiliates) and 20(f)(Subcontracting and Assignment) of the Agreement do not apply to the Affiliate.
- 5. The Affiliate agrees that it may not enforce the Agreement against Epic and that any remedies available against Epic may only be enforced by AHS.
- 6. The Affiliate agrees and acknowledges that as between the Affiliate and AHS, and notwithstanding any other provision of the Agreement, AHS shall have no liability for the Affiliate’s use of the Program Property. The Affiliate shall indemnify and hold AHS harmless from and against any Claim brought against AHS or its Indemnitees arising out of a breach of the Agreement by the Affiliate or its End Users, or otherwise resulting from, or in connection with the Affiliate’s or its End Users’ use of the Program Property and any Damages therefrom.
- 7. Capitalized terms used in this Acknowledgement shall have the same meaning as in the Agreement unless otherwise defined herein.
- 8. This Acknowledgement comes into effect as of the Effective Date and shall remain in effect for so long as the Affiliate is using any Program Property unless the Affiliate’s access to Program Property is terminated earlier or the Agreement is terminated.

IN WITNESS WHEREOF the undersigned has caused this Acknowledgement to be executed by its duly authorized representatives on the dates set forth below.

[Please Print Full Name of Individual above this line]

Signature: _____

Date: _____

Schedule B
Provider/Affiliate Information
(please complete)

Provider Name:

Lead Custodian:

Alternate Lead Custodian:
(Optional)

Access Administrator:

Please complete the following table for yourself and any Authorized Staff who will require access to CCPP as of the Effective Date. Any changes to this list after the Effective Date need to be managed using current AHS Identity & Access Management (IAM) protocols.

<u>Data Attribute:</u>	<u>Purpose for Collection:</u>	<u>Please Complete and do not abbreviate</u>
Full First Name, Middle Name, Last Name	Identifies the name of the user to convert user login to human readable reporting	
Job Title	User job title is required to determine appropriateness of access	
User Role	User Role is required to determine appropriateness of access (examples, Nurse/Doctor/Analyst/MOA etc.)	
Name of Organization you work for	Organization the User is affiliated with. Required to assist in identifying same organization co-workers and to assist with proper investigation routing and reporting; e.g., AHS, APL, Covenant, Carewest etc.	
User Facility Address(es)	Address(es) of facility work location. Required to determine appropriateness of access. (If multiple must be listed separately). Street address, city, province, postal code.	
Organization uses Connect Care as their Own EMR	If the Organization has an agreement to use Connect Care as their own legal record of care please indicate YES , otherwise respond NO	
Department	The department of the organization the User is associated with. Required to determine appropriateness of access and convert to human readable reporting (I.e. Working out of AHS cardiac department).	
Manager Name	Who oversees the User for employee or contract management purposes. Required to assist with possible further investigations as required (i.e. who you report to)	
Manager Email	Email address of manager listed above. Required to assist with possible investigations and notification purposes. (Please provide the Manager's primary <u>active</u> email for notice purposes).	

Hire Date	User Hire date. Required to determine appropriateness of access.	
Termination Date	User Termination date. Required to determine appropriateness of access. To be updated/completed/submitted at time of termination. Leave blank until known.	
User Status	Status of position for user. Required to assist in determining scheduling and appropriateness of access Choose from: Active, Terminated, On leave.	
User Category	Choose from: Physician, Affiliate to AHS, Affiliate to Physician, other (please identify) Required to classify the User for appropriate access and investigation path, if necessary.	
User Type	Identifies position category of User. Required to assist in determining scheduling and appropriateness of access Choose from: Full-time, Part-Time, Contract	
DOB	Day, Month, Year of User's birth. Required to support auditing alerts and investigations or self-access.	
User Home Address 1	Physical User home address (including city, province, postal code). Required to assist with determination of appropriateness of access. (Street, city, province, postal code).	
User Email Address	Primary Current email address of User. Required to assist with possible further investigation.	
Zone	AHS Zone of User. Choose from North, Edmonton, Central, Calgary, South. Required to assist with proper investigation routing and reporting.	
Dual Employee/Role	Yes or No descriptive field – User has more than one employment role (i.e. Covenant Employee and Lab Tech; AHS and PCN employee working AHS facility etc., Clinic employee and AHS Employee)	

PLEASE RETURN A SIGNED, COMPLETED COPY OF THE AGREEMENT TO:

Alberta Health Services
c/o Ambulatory Support Team at the following address
ccproviderportal.access@ahs.ca

EPIC AFFILIATE USER ADDENDUM FAQ

Note: This FAQ is intended for informational purposes only to assist with your understanding of the Affiliate User Addendum and is not intended to be contractually binding. This FAQ is AHS' Confidential Information.

What is the Epic Affiliate User Addendum (Epic Addendum)?

Epic Systems Corporation ("Epic") is the technology company that developed the proprietary technology that AHS uses for the CCPP. The Epic Addendum is a one-page agreement signed by each Custodian at the same time as the CCPP Access Agreement. The Epic Addendum requires the Custodian to provide Epic with direct assurance that as an end-user of Epic's technology, the Custodian will comply with the agreement between Epic and the Custodian to the extent the terms apply to Custodian's use of the CCPP.

These terms are typical of any software license agreement. The following high-level summary describes what this means for you and your Authorized Staff. Many of these obligations are already included in the CCPP since they represent best practice for managing confidential information in general.

- Only use the CCPP for the provision of health care services
- Protect Epic's proprietary and confidential information. For example, you cannot share screenshots of the Epic software, data structures, Epic user guides or other Epic confidential and proprietary information made available to you by AHS or found in the CCPP
- Don't share Epic's proprietary and confidential information with Epic's competitors
- Don't remove Epic's trademark and copyright notices from Epic materials
- Contact AHS for further direction if you want to create any training materials for the CCPP
- You and your Authorized Staff are only end users of the CCPP. As end users, you won't try to find out the source code of the CCPP or try to do software programming for the CCPP without Epic's and/or AHS' consent
- You need to contact AHS to get further direction if you want to integrate the CCPP with other technology
- You should use confidentiality agreements protecting third party proprietary and confidential information with personnel working in the Clinic. If you discover a breach of confidentiality of the Epic proprietary and confidential information, notify AHS immediately
- If for some reason you get a request for information about the CCPP under freedom of information legislation, contact AHS immediately
- If you have problems with the Epic technology in the CCPP, call AHS don't call Epic
- If you engage a third party who will be provided access to Epic proprietary and confidential information you must contact AHS first for further direction
- When in doubt, call AHS with any questions you may have about the Epic Addendum

Who do I contact if I have questions about the Epic Addendum?

If you have any questions about the Epic Addendum please send them to the following:

Ccproviderportal.Access@albertahealthservices.ca.

APPENDIX 4

ANP Role		CCPP		Difference
Role	Users	Role	Users	Explanation
Clinical 1	Physicians, Nurse Practitioners	CCPP Provider	Physicians, Nurse Practitioners	<ul style="list-style-type: none"> The same users
Clinical 4	Nurses, LPN's, rarely clinicians in DI clinics	CCPP Clinical MOA	MOA Support (regulated professionals): Nurses, LPN's	<ul style="list-style-type: none"> CCPP differentiates access required for clinical staff that are governed by a regulated health profession Regulated Healthcare professionals (for example, LPN that report to a medical professional association) are accountable to their association CCPP does not include DI clinic staff as this user requires different access. A future role may include this user type
Clinical 8	Clinical staff, registration staff, HIM, UofC MOA	CCPP Admin – Clerical MOA	MOA Support (non-regulated professionals): MOA's, general admin	<ul style="list-style-type: none"> CCPP differentiates provider support staff that are not part of a regulated health profession to align with their scope of practice Graduate of a college and has taken medical reception and now been trained by the physician to do additional work for them in their clinic and they don't have that regulated status

CCPP via ANP Onboarding and Offboarding Processes

The Connect Care Provider Portal (CCPP) is a web-based application that allows non-AHS clinicians with appropriate role-based access to securely access the health information in Connect Care.

It is designed to improve the continuity of care for patients as they move between sites in AHS that use Connect Care and their primary care providers in the community using a private Electronic Medical Record. Clinicians who currently use the Alberta Netcare Portal (ANP) will be able to access the CCPP via an in-context launch from a link in the ANP. This should facilitate access while allowing AHS to fulfill its obligations under the Health Information Act. Given AHS is the custodian of this health record, it must meet the obligations of the Health Information Act to ensure the privacy and security of access to the record.

This document is intended to provide a comprehensive overview of the onboarding and offboarding processes for community providers who request access to CCPP via ANP. It covers the different steps involved in the onboarding process, including the information required by AHS Teams and end users. It also outlines the offboarding process and provides guidance on how to ensure that all data is securely removed from the portal. We have aimed to streamline the onboarding process by mirroring the existing obligations of providers to access ANP as closely as possible. If at any time you have questions or concerns, please reach out to ccproviderbridge@ahs.ca.

Definitions

Below are the definitions of the specific roles/key terms involved in the onboarding and offboarding process. Depending on the size and make up of a clinic, a single individual may play multiple roles. It is important to understand that each person who accesses CCPP must be identified as a specific role (see table below).

ANP Role		CCPP		Difference
Role	Users	Role	Users	Explanation
Clinical 1	Physicians, Nurse Practitioners	CCPP Provider	Physicians, Nurse Practitioners	<ul style="list-style-type: none">Roles are equivalent
Clinical 4	Nurses, Licensed Practical Nurses (LPNs), rarely clinicians in Diagnostic Imaging (DI) clinics	CCPP Clinical Support	Nurses, LPNs	<ul style="list-style-type: none">CCPP differentiates access required for clinical staff that are governed by a regulated health professionRegulated Healthcare professionals (for example, LPN that report to a medical professional association) are accountable to their associationCCPP does not include DI clinic staff as this user requires different access. A future role may include this user type

ANP Role		CCPP		Difference
Role	Users	Role	Users	Explanation
Clinical 8	Clinical staff, registration staff, HIM, MOA	CCPP Admin – Clerical MOA	MOA Support (non-regulated professionals) : MOA's, general admin	<ul style="list-style-type: none"> • CCPP differentiates provider support staff that are not part of a regulated health profession to align with their scope of practice • Graduate of a college and has taken medical reception and now been trained by the physician to do additional work for them in their clinic and they don't have that regulated status

Other Definitions

Access Administrator – This role can be performed by the Lead Custodian (see below) or can be assigned to a person identified by the Lead Custodians as a delegate. This role manages the day-to-day access issues for the clinic, for example an Office Manager or Nurse. The Access Administrator (if any) is responsible for submitting requests for the Authorized Staff, they may also support the Lead Custodian to complete the required documentation, but they cannot sign any of agreements and other documents required to get access to the CCPP on the clinic's behalf. Signing any privacy and security documents related to the CCPP must be done by the Lead Custodian.

Affiliate of a Custodian – An affiliate is fully defined in the Health Information Act (1(1)(a). For the purposes of the CCPP and in the community clinic settings the affiliates, in relation to the custodian means (i) an individual employed by the custodian, (ii) a person who performs a service for the custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian.

Authorized Staff – Support staff at the clinic who are identified in a clinic's CCPP access agreement.

CCPP Ambassador – CCPP Ambassadors offer concierge-type service to any interested CCPP users. Ambassadors are responsible for explaining and ensuring eligibility requirements of the CCPP and facilitating all onboarding requirements.

Clinic – For the purpose of the CCPP, a clinic is the location, environment, or other work arrangement (such as a remote service delivery model) where a Custodian and Authorized Staff provide health services.

Custodian – The HIA defines who is a Custodian of health information. AHS, physicians, registered nurses, pharmacists, and midwives are examples. Any party who signs the CCPP Access Agreement must be a Custodian because the HIA permits disclosing health information between Custodians. Custodians must also take responsibility for their own staff who are considered their affiliates under the HIA.

Lead Custodian – The Lead Custodian is the primary Custodian to carry out the compliance obligations under the CCPP Access Agreement. A Lead Custodian does not have to be the same person who is identified as the Lead Custodian for the local EMR or for Netcare. Lead Custodians manage compliance issues for a clinic. The Lead Custodian can also perform the Access Administrator role.

Alberta Netcare Permission Matrix

As outlined in Section 5.1 of the [Health Information Act \(HIA\)](#), authorized custodians are permitted to share and access prescribed health information through Alberta Netcare, facilitating the secure exchange of health information among healthcare providers.

To maintain the protection and privacy of individual health information, custodians and affiliates can only collect, use and disclose health information in the most limited manner, with the highest degree of anonymity possible and on a need-to-know basis. As such, the Alberta Netcare Permission Matrix identifies the level of access to Alberta Netcare based on Alberta Netcare user role.

User Roles

The matrix lists the Alberta Netcare user roles, also referred to as “user roles,” under the following broad categories:

- **Administration:** Access to Person Directory (PD) and other functions, no access to clinical data or Pharmaceutical Information Network (PIN)
- **Clinical:** Access to various clinical data, PD, PIN and Connect Care Provider Portal (CCPP)
- **Pharmacy:** Access to various clinical data, PD and PIN

NOTE

Pharmacies engaged with Real-Time Integration (RTI) through their vendor system must select the option PIN Dispense if it is not automatically included with the user role selected.

These categories do not necessarily align to a specific type of profession or job role but do identify that there is varying access to information and functionalities (e.g. prescribe, dispense, update, create) from one Alberta Netcare role to the next.

All roles have standard access (Y) which is automatically provisioned when the role is selected. Most Clinical and Pharmacy roles also have optional access (O) which must be manually selected before it will be provisioned. Information or functionalities that are not available to a role is identified with a (N).

Other roles are restricted to certain types of users:

- **Clinical 1** is for users who are licensed by the College of Physicians & Surgeons of Alberta (CPSA) or College of Registered Nurses of Alberta (CRNA) and have prescribing rights.
- **Clinical 2** is typically assigned to nurses, medical office assistants, and Office of the Chief Medical Examiner (OCME) users.
- **Clinical 10** is typically selected for users that are licensed by the Alberta College of Optometrists (ACO) or College of Dental Surgeons of Alberta (CDSA).
- **Clinical 11** is typically selected for Lloydminster Hospital.
- **Clinical 12** is typically selected for users that are licensed by the College of Chiropractors of Alberta (CCOA).
- **Pharmacy 2** is for users that are licensed by the Alberta College of Pharmacy (ACP).

Portal Groups

Alberta Netcare Portal (ANP) is a viewer into patient EHRs, and provides key health information such as demographics, event history, lab results, immunizations, transcribed reports, community reports and medications.

For more information on ANP, visit the [Alberta Netcare Learning Centre](#).

Portal																	PIN	PD			CCPP					
User Roles	Groups																View	Prescribe	Dispense	View PD	Update PD	Update Newborn	View Newborn	View CCPP		
	Demographics																									
	Patient Search																									
	Patient Lists																									
	Limited Patient Search																									
	Favourites																									
	Access PD																									
	Access PIN																									
	Document Forwarding																									
	Messaging																									
	Lab																									
	Event & Immunization History																									
	Transcribed Reports																									
	DI Reports and Images																									
	Clinical Documents																									
eReferral Create																										
eReferral Create on Behalf of & Edit																										
eReferral View																										
eReferral Notifications																										

Demographics	Provides access to patient demographic information. (i.e. PHN, first and last name, age, address and phone number(s).
Patient Search	Allows users to search by Patient Demographic Information (e.g. Name) or by Patient Identifier (e.g. PHN).
Patient Lists	Current lists of patients in an AHS Edmonton facility that meet pre-defined search criteria. Provider Patient List returns all patients for a specified provider.
Limited Patient Search	Limits user search criteria to Patient Identifier (e.g. PHN)
Favourites	Patient Search includes a favourite search function where users can save the name or PHN/ULI of patient records that you access on a regular basis.
Access PD	Provides community patient person-identifiable demographic information
Access PIN	Provides community patient medication information
Document Forwarding	Enables authorized users to email a selected ANP Clinical Document to another ANP user. The recipient requires the appropriate User Role to view the document.
Messaging	ANP's messaging feature enables secure communication between ANP users.
Lab	Allows viewing of patient lab test results
Event & Immunization History	Patient Event History (Hospital visits) summarizes a patient's contact with AHS facilities. The Immunization History summarizes a patient's immunizations.
Transcribed Reports	Allows the viewing of transcribed medical reports including: <ul style="list-style-type: none"> admission histories discharge/transfer summaries consultations operative/procedure reports community encounter digests specialized reports from Cancer Centres
DI Reports & Images	Diagnostic Imaging (DI) reports are transcriptions from the radiologist who examined the images. Diagnostic Imaging includes X-rays, MRIs, ultrasounds and CT scans.
Clinical Documents	User role determines what clinical documents can be accessed through the Clinical Document Viewer (CDV) (e.g. Lab; Transcribed Reports, Diagnostic Images, etc.)
eReferral Create	Displays the Request for Service screen to create a referral, and lists all referrals; Drafts, In Progress and Completed or Cancelled or Declined
eReferral Create on Behalf of & Edit	Allows users to manage referrals on behalf of a providers they are associated with through their My Details
eReferral View	Displays all referrals; Drafts, In Progress and Completed, Cancelled, or Declined
eReferral Notifications	Allows users to subscribe to email notifications related to their eReferrals

PIN Groups

PIN is the central repository for patient medication information. It offers access to pharmacy care plans, drug monographs, decision support, dispense data, allergy/intolerance information, and prescription management within ANP.

For more information on PIN, visit the [Alberta Netcare Learning Centre](#).

Portal																			PIN	PD			CCPP
User Roles	Groups	Demographics	Patient Search	Patient Lists	Limited Patient Search	Favourites	Access PD	Access PIN	Document Forwarding	Messaging	Lab	Event & Immunization History	Transcribed Reports	DI Reports and Images	Clinical Documents	eReferral Create	eReferral Create on Behalf of & Edit	eReferral View	eReferral Notifications				
		View	Prescribe	Dispense	View PD	Update PD	Update Newborn	View Newborn															

Provide access to a patient's medications via PIN which includes:

- medications (active/inactive)
- allergy and intolerance information
- pharmacy care plans
- drug monographs
- drug decision support
- dispense information
- prescription creation
- drug warning management

View	Allows users to view the patient's medications through PIN and Medication Profile
Prescribe	Allows users to create new/renew prescriptions, change prescription status, correct a prescription, and augment medication instructions
Dispense	Allows the dispense of a patient prescription, and other dispense activities

PD Groups

PD provides access to demographic and Alberta Health Care Insurance Plan (AHCIP) eligibility information within ANP. For more information on PD, visit the [Alberta Netcare Learning Centre](#).

Portal																				PIN	PD			CCPP
User Roles	Groups	Demographics	Patient Search	Patient Lists	Limited Patient Search	Favourites	Access PD	Access PIN	Document Forwarding	Messaging	Lab	Event & Immunization History	Transcribed Reports	DI Reports and Images	Clinical Documents	eReferral Create	eReferral Create on Behalf of & Edit	eReferral View	eReferral Notifications					
		View	Prescribe	Dispense	View PD	Update PD	Update Newborn	View Newborn	View CCPP															

- search for a person (by additional demographic criteria)
- view patient demographic information
- check eligibility for health care coverage
- add or update a person's demographic information
- merge duplicate PHNs

View PD	Provides access to person-identifiable demographic and AHCIP eligibility information
Update PD	Allows users to update patient information within PD (except Newborn)
Update Newborn	Allows users to update Newborn information within PD
View Newborn	Users can view Newborn information within PD

CCPP (Connect Care Provider Portal)

CCPP enables authorized ANP users to securely view Connect Care patient information, providing them with a more complete view of a patients health care information.

For more information on CCPP, visit the [Alberta Netcare Learning Centre](#).

Portal																	PIN	PD	CCPP							
User Roles	Groups																									
	Demographics	Patient Search	Patient Lists	Limited Patient Search	Favourites	Access PD	Access PIN	Document Forwarding	Messaging	Lab	Event & Immunization History	Transcribed Reports	DI Reports and Images	Clinical Documents	eReferral Create	eReferral Create on Behalf of & Edit	eReferral View	eReferral Notifications	View	Prescribe	Dispense	View PD	Update PD	Update Newborn	View Newborn	View CCPP

CCPP Permissions

The following maps the Alberta Netcare roles to the CCPP role.

Netcare User Type	Netcare Role	Typical Profession role	CCPP User Type	CCPP Roles
Custodian	Clinical 1	Medical Doctor, Naturopathic Doctor, Nurse Practitioner	Provider	CP
Custodian Affiliate – Regulated Profession	Clinical 2	Certified Graduate Nurse, Licensed Vocational Nurse, Registered Midwife, Registered Nurse, Licensed Practical Nurse	Regulated Clinical Support	CR
Custodian Affiliate - Non-regulated profession	Clinical 2	Medical Office Assistant (MOA)	Non-regulated Clinical Support	CN
AH Affiliate OCME	Clinical 2	Medical Examiner (ME) / ME Investigator	Regulated Clinical Support	CR

Refer to the **Connect Care Provider Portal (CCPP) User Roles and Access Table (version 1.0)** within the matrix document to identify the user role access.

Patient search - Full (first access)	Enables full patient search function
Patient search (limited ULI & DOB)	Enables limited ULI & DOB search
Facesheet	Ability to view patient facesheet
Storyboard	Ability to view patient storyboard
Patient snapshot (high level summary)	Enables users to view the Patient Snapshot – a high level summary of patient information
Patient chart advisories	Ability to view various patient chart advisories. <ul style="list-style-type: none"> CCPP roles have limited access to certain patient chart advisories (e.g., identity theft). CCPP roles are required to 'Break-The-Glass' (BTG) to access the following specific advisories . BTG is triggered at 2 levels. <ul style="list-style-type: none"> Patient Level Encounter Level The CP user role can access sensitive notes for physicians with specialty match.
Upcoming appointments	Ability to view upcoming appointments
Referrals (view)	Ability to view referrals

Notes (view)	Ability to view notes entered by other providers
Laboratory results	Ability to view laboratory results
Imaging results	Ability to view imaging results
Medication (view only)	Ability to view medications
Letters	Ability to view letters
Messaging (In basket)	Enables users to send and receive messages
Demographics	Ability to view patient demographics
Care team	Ability to view the patient care teams
Allergies	Ability to view allergies
Medication activity	Ability to view medication activity
Chart search	Enables users to search patient charts

Business Requirements

CCPP via ANP

Ministry

Alberta Health

Division Name:

Health Information Systems

Branch/Unit:

Strategic IMT Services

Creation Date:

October 1, 2024

Print Date:

December 13, 2024

Document Version:

1.0

Template Location

Primary Contact:	Project Management Office (PMO)	Health.PMO@gov.ab.ca
Template Location:	The master copy of this template is located in the PMO Framework HealthShare Site.	
Template Version	V 1.0.2	
Template Date	May 28, 2014	

Template Usage

This template is being provided by Alberta Health through the PMO, Information Management Branch of Health Information Systems (HIS) Division to provide a common and consistent approach for the delivery of IT-related initiatives and projects.

Some sections of the template may contain *italicized* descriptive information that should be removed once the template has been filled in.

Some projects may require additional elements be added to the deliverable, additional elements may be inserted throughout the document as appropriate. **Note: Removing template sections may introduce risk and potentially affect the success of the project. In the event that a section is not applicable to your project, a brief explanation should be provided as to why it is not applicable.**

Deliverables should wherever possible, be provided in MS Word format. Embedded objects such as diagrams and charts should be created using a common or standard tool such as MS Word and MS Visio and the source objects should be available rather than just a snapshot of the objects.

Your opinion and suggestions for improving this template are important to the PMO, Health Information Systems Division (HIS). The PMO has instituted a review and release process to help improve the templates. Contact the PMO to learn how your input to continuous improvement can be captured.

Table of Contents

DOCUMENT LOCATION	4
DOCUMENT REVISION HISTORY	4
DELIVERABLE APPROVERS AND REVIEWERS	4
1 DOCUMENT PURPOSE.....	6
1.1 BACKGROUND	6
1.2 CURRENT STATE	6
1.3 TARGET STATE.....	6
2 BUSINESS CONTEXT	8
2.1 BUSINESS DRIVERS.....	8
2.2 BUSINESS OBJECTIVES.....	8
3 REQUIREMENTS	9
3.1 BUSINESS REQUIREMENTS	9
3.2 SYSTEM REQUIREMENTS.....	10
3.3 INFORMATION SECURITY REQUIREMENTS	10
3.4 DESIGN REQUIREMENTS	10
3.5 TRAINING REQUIREMENTS	11
3.6 AUDITING REQUIREMENTS	12
3.7 CCPP REQUIREMENTS FOR CUSTOMER RELATIONSHIP MANAGEMENT (CRM).....	13
3.7.1 Facility Requirements.....	13
3.7.2 User Requirements.....	14
3.7.3 Case Management Requirements.....	14
3.8 SUPPORT FOR CCPP USER.....	17
4 TERMS, ACRONYMS, AND ABBREVIATIONS	20
5 REFERENCES	21
6 APPENDIX A: CONCEPT OF OPERATION.....	22

Document Location

Document Revision History

Version	Version Date	Summary of Changes	Author
0.1	October 1, 2024	Initial Draft	Lisa Cloutier
0.2	October 29, 2024	Revised based on feedback from AH and AHS	Lisa Cloutier
0.3	November 5, 2024	Revised based on feedback from AH and AHS	Lisa Cloutier
0.4	November 8, 2024	Revised based on feedback from AH and AHS	Lisa Cloutier
0.5	November 25, 2024	Revised based on feedback from AH and AHS	Lisa Cloutier
0.6	December 5, 2024	Revised based on feedback from AH and AHS	Lisa Cloutier
0.7	December 10, 2024	Revised based on feedback from AH and AHS	Lisa Cloutier
1.0	December 13, 2024	Final Version	Lisa Cloutier

Deliverable Approvers and Reviewers

Use the following table to name the deliverable approvers and reviewers. Deliverable approvers and reviewers should be the same as those already stated in the Project Management Plan for this deliverable.

Title and Name	Type	Purpose
Todd James Director, Consumer eHealth, AH	A	Reviews and approves
Lisa Brower Director, HIA Policy, Privacy and Security, AH	A	Reviews and approves

Title and Name	Type	Purpose
Lloyd Thorpe Senior Project Manager, eHealth Ecosystem Modernization, AH	A	Reviews and approves
Ryan Zimmerman Senior Project Manager, Health Information Continuity, Provincial Primary Health Care, AHS	A	Reviews and approves
Stephen Smithbower Director, Health Information Continuity, Provincial Primary Health Care, AHS	A	Reviews and approves
Sharon McNaughton IT Senior Analyst, Ambulatory, EMR and Portals Connect Care, AHS	R	Reviews
Desiree Fadri Senior Consultant, Health Information Continuity, Provincial Primary Health Care, AHS	R	Reviews
Verica Jelic EHR Deployment Manager, AH	A	Reviews and approves
Sheri Ross Senior Clinical Specialist, AH	A	Reviews and approves
Amanda Harrigan Policy Advisor HIA, AH	A	Reviews and approves
Rorisang Hlahatsi-Baloyi Senior Management Consultant, Emerging Technology, CGI	R	Reviews
Tara England Director, Consulting Services, eHS Operations Manager, CGI	R	Reviews
Abdul Lawal Director, Consulting Services, eHS Account Manager, CGI	R	Reviews

Type: A – Approves (implies review as well); P – Prepares; R – content review and input; I – Information Only

1 Document Purpose

The purpose of this document is to define the requirements for mixed context providers and their staff and Office of Chief Medical Examiner (OCME) staff to request access to Connect Care Provider Portal (CCPP) via Alberta Netcare Portal (ANP).

This deliverable captures business requirements, system requirements, information security requirements, design requirements, training requirements, auditing requirements, CCPP requirements for Customer Relationship Management (CRM), CCPP Support requirements and business rules.

The objective of defining requirements is to obtain a clear understanding of the business processes, rules, functions, and information required to meet the business objectives.

1.1 Background

The Connect Care Provider Portal (CCPP) is a web-based application that allows clinicians and staff (from community sites and OCME) with appropriate role-based access to securely access the health information from Connect Care, making more complete information available when a patient seeks treatment. Alberta Health and Alberta Health Services have been working together to enable community providers to access the CCPP via Alberta Netcare. The CCPP button in Netcare was released in January 2022 allowing Netcare users with Connect Care authorized access to launch the CCPP from Netcare Portal.

1.2 Current State

Currently, providers who work both within AHS and their community clinical practice, referred to as 'mixed context providers' (AHS affiliates), may have Connect Care access through Hyperdrive when working at the AHS site, but when working at the community site these providers, as well as their staff in the community practice, do not and required patient follow up is challenged as a result.

Currently, users in the OCME have Netcare access but do not have CCPP access.

1.3 Target State

The Connect Care Provider Portal would allow an Authorized Custodian with ANP access to log into Netcare and to access the CCPP via an in-context launch from a tab in ANP. Once within Connect Care, the user can search for records of other patients.

Deploying CCPP access to providers and their office staff will support the providers and improve both patient care and health informational continuity. To ensure continuity of care and access to required health information, Alberta Health is asserting control over the CCPP. By assuming direct control over CCPP, Alberta Health will rely upon authorities that it has as the Ministry of Health under the Health Information Act which are not available to AHS.

The primary CCPP project focus is the deployment of CCPP to community providers and their clinic staff with the initial focus on mixed context providers. Leveraging existing Netcare Portal processes for onboarding users, processes will be defined for community providers to request

and manage access to the CCPP. Operational processes to support users through the process will also be established.

A secondary project focus is the deployment of CCPP to OCME users with Netcare access. This initiative will involve adapting existing onboarding processes to cater specifically to OCME users, ensuring they can effectively request and manage access to the CCPP system. Operational workflows will be defined to support these users, facilitating a smooth integration of CCPP into their daily practices. Additionally, tailored training and support resources will be established to empower OCME staff, ensuring they are equipped to utilize CCPP effectively in their roles.

In order to allow the sharing of EPIC information between AHS and CGI an EPIC Access Agreement needs to exist. This is in progress, AH is in discussions with HIAPPSU, CGI and AHS - ETA Dec 17/24.

2 Business Context

2.1 Business Drivers

To improve the continuity of care for patients as they move between sites in AHS that use Connect Care and their primary care providers in the community.

To improve access to information required by the OCME to support decision-making and fatality investigations.

2.2 Business Objectives

The objective of this project is to establish standardized processes for granting and managing access to CCPP via ANP for both Lead Custodians (mixed context providers) and their associated community clinic staff. These processes will ensure seamless continuity of patient care. Additionally, the project will define processes for granting and managing CCPP access via ANP for ANP users within the OCME.

3 Requirements

3.1 Business Requirements

The Business Requirements are as follows:

1. For the current implementation, deployment should enable CCPP access for mixed context providers and their staff. Three CCPP roles have been defined which include physicians and nurse practitioners (prescribers), nurses (support staff – regulated professional) and medical office assistants or other clinical support staff (support staff – non-regulated). The Connect Care Provider Portal already exists today, and the CC Provider Portal button is already in ANP therefore the requirement is for the CC Provider Portal button to be enabled for mixed context providers and their staff once all other requirements have been met. At the present time there is a change request to have the name of the button within ANP changed from “CC Provider Portal” to “CCPP”, but this change will not be implemented until March 2025 at the earliest.
2. ANP PIA will be amended with CCPP via ANP addendum.
3. The Netcare Access Administrator (AA) must be able to enter the CCPP entitlement, as appropriate, into AHS IAM.
4. The community clinics need to be using AHS IAM for managing staff access to Netcare to be able to request CCPP access for their staff (WDFA will be on the AHS IAM rollout list). Their Netcare AA would be setup with access to AHS IAM and would use the existing ANP entitlement request workflow to request optional access to CCPP.
5. CCPP must be available for OCME in Phase 1 – items to consider:
 - Review Memorandum of Understanding (MOU) to determine if amendments are required to accommodate for CCPP
 - Involves paper-based Netcare URF's and there is no override functionality for the approval process for CCPP
 - When paper-based Netcare User Registration Forms (URF's) are used and the staff are not in AHS IAM, the processor of the URF (HIAPPSU) would submit a request in AHS IAM. Currently HIAPPSU is the Authorized Approver for OCME User Netcare access.
 - For OCME Users, the Netcare URF will need to be amended to add the optional checkbox for CCPP
 - The connection/dependency between the ANP user role and the CCPP user role is still to be determined
6. Precondition: An EPIC Access Agreement needs to be in place between EPIC and CGI to allow the sharing of the EPIC information.
7. CCPP 180-day Inactive Access Account Disabling functionality is required. CCPP Access Certification is not required.
8. If the Netcare Access Administrator (NAA) goes directly to AHS IAM to submit a CCPP access request (bypassing eHS), when the CCPP request is submitted an automated email notification will be sent to an eHS shared mailbox (eHealthPrivacy@gov.ab.ca) so steps can be built to support eHS review of PIA and pORA to ensure all privacy and security

requirements have been met and to ensure the CCPP Access Agreement has been completed for each Custodian at the community site.

3.2 System Requirements

The System Requirements are as follows:

1. The OCME, mixed context provider and staff need to have ANP access prior to accessing CCPP.
2. The appropriate roles must exist within AHS IAM prior to CCPP access being granted.
3. The ANP roles will need to be mapped to the appropriate CCPP roles.
4. The current Netcare Permission Matrix will identify CCPP required permissions mapped to the existing Netcare roles. ANP matrix will be linked to the CCPP permissions depend on the level of access needed.

3.3 Information Security Requirements

The Information Security Requirements are as follows:

1. An AD account will need to be created for all Community users prior to accessing CCPP. An AD group is required to authenticate the CCPP user into the provider portal.
2. For mixed context providers there will be two AD groups set up because when working at the AHS facility, they will access Connect Care through Hyperdrive whereas when they are working at the community facility, they will access Connect Care Provider Portal.
 - When accessing Connect Care through Hyperdrive the AHS.EpicConnectCare.EndUsers Connect Care group will be used
 - When accessing Connect Care Provider Portal the AHS.EpicConnectCare.ProviderPortal CCPP group will be used
3. The requestor must have an RSA token to access the AHS Epic (Connect Care) Information questionnaire (Smart Auditing Tool). The AHS Epic (Connect Care) Information questionnaire is accessed within AHS IAM using the self-service menu. This should not be an issue as RSA tokens are required for Netcare ANP access. Soft tokens are the default option to be selected.

3.4 Design Requirements

The Design Requirements are as follows:

1. Since Phase 1 involves OCME, mixed context providers and their staff, the CC Provider Portal (CCPP- after March 2025) button within ANP will not be enabled for others and there must be appropriate messaging put into place to notify those Netcare Users. To meet this requirement the messaging that will be displayed when the CC Provider Portal (CCPP- after March 2025) button is selected within ANP will be displayed as follows:

Thank you for your interest in Connect Care Provider Portal (CCPP). The CCPP provides information about treatment and care your patients receive from AHS facilities. With CCPP you can improve the continuity of care for your patients. You are not

currently registered for CCPP access. If you would like to apply for access or need more information about CCPP, please contact:

eHealth Netcare Provider Support
Phone: 1-855-643-8649
Email: eHealthProviderSupport@gov.ab.ca

For more information copy the link and paste into your browser:
www.ahs.ca/ccproviderportal

This messaging has been approved by AH and AHS.

This messaging will be put in place for Limited Production Rollout (LPR) and will be revisited after LPR.

2. Currently within ANP the CC Provider Portal button is labelled “CC Provider Portal”. At the present time there is a change request to have the name of the button within ANP changed from “CC Provider Portal” to “CCPP”, but this change will not be implemented until March 2025 at the earliest.
3. Information within CCPP will be view only.

3.5 Training Requirements

The Training Requirements are as follows:

1. Each CCPP user must provide a valid personal/work email address prior to accessing MyLearning Link. The email address is part of the Epic (Connect Care) Information questionnaire that is entered within AHS IAM.
2. Mandatory training such as: *OOBB – On Our Best Behavior* and *Introduction to CCPP video*, must be completed prior to CCPP access being granted to the user. This applies to any provider accessing CCPP. All providers as well as their staff and OCME users, requesting CCPP access via ANP, must complete these two mandatory training.
3. The CCPP training will exist within the MyLearning Link application. OCME and community users will need access to MyLearning Link when the CCPP request is received in order to take the OOBB and Introduction to CCPP training.
4. Currently the training is offered within MyLearning Link (MLL). When a request for CCPP comes in, an AD account is created, and as a part of the EPIC workflow the user and NAA will receive an automated email from the AHS IAM system indicating a role has been assigned to the user, outlines the associated training required and contains the MLL link to allow access to the training. Once the training is completed AHS LDAP is notified from MLL. Tableau queries MLL every 4 hours and pulls back all training results. The MLLTrainingTrack field in AHS LDAP is then directly updated to completed and the completed status is pushed to AHS IAM. When it is detected AHS IAM provisions access for the template/role that was associated. Once the role is provisioned AHS IAM changes the status of the role in AHS LDAP to provisioned (alternate statuses are cancelled, revoked and retrain).
5. CCPP Training will not be tracked by eHS.

3.6 Auditing Requirements

The Auditing Requirements are as follows:

1. User attributes need to be defined to support the Smart Auditing Tool during the CCPP Onboarding process to monitor access events. These are as follows:

The following chart identifies the user attributes collected to flag suspicious activity as defined by the Enforced Policies.

User Attributes:	Purpose for Collection:
Full First Name, Middle Name, Last Name	Identifies the name of the user to convert user login to human readable reporting
Job title	User job title is required to determine appropriateness of access
User role	User role is required to determine appropriateness of access (examples, Nurse/Doctor/Analyst/MOA etc.)
Name of organization the user works for	Organization the User is affiliated with. Required to assist in identifying same organization co-workers and to assist with proper investigation routing and reporting, e.g., AHS, APL, Covenant, Carewest etc.
User facility address(es)	Address(es) of facility work location. Required to determine appropriateness of access. (If multiple must be listed separately). Street address, city, province, postal code.
If the organization uses Connect Care as their own CIS	If the organization has an agreement to use Connect Care as their own legal record of care please indicate YES, otherwise respond NO
Department	The department of the organization the User is associated with. Required to determine appropriateness of access and convert to human readable reporting (i.e. Working out of AHS cardiac department).
Manager Name	Who oversees the User for employee or contract management purposes. Required to assist with possible further investigations as required (i.e. who you report to)
Manager Email	Email address of manager listed above. Required to assist with possible investigations and notification purposes. (Please provide the Manager's primary <u>active</u> email for notice purposes).

Hire Date	User Hire date. Required to determine appropriateness of access.
Termination Date	User Termination date. Required to determine appropriateness of access. To be updated/completed/submitted at time of termination. Leave blank until known.
User Status	Status of position for user. Required to assist in determining scheduling and appropriateness of access. Choose from: Active, Terminated, On leave.
User Category	Choose from: Physician, Affiliate to AHS, Affiliate to Physician, other (please identify) Required to classify the User for appropriate access and investigation path, if necessary.
User Type	Identifies position category of User. Required to assist in determining scheduling and appropriateness of access. Choose from: Full-time, Part-Time, Contract
DOB	Day, Month, Year of User's birth. Required to support auditing alerts and investigations or self-access.
User Home Address 1	Physical User home address (including city, province, postal code). Required to assist with determination of appropriateness of access. (Street, city, province, postal code).
User Email Address	Primary Current email address of User. Required to assist with possible further investigation.
Zone	AHS Zone of User. Choose from North, Edmonton, Central, Calgary, South. Required to assist with proper investigation routing and reporting.
Dual Employee/Role	Yes or No descriptive field – User has more than one employment role (i.e. Covenant Employee and Lab Tech; AHS and PCN employee working AHS facility etc., Clinic employee and AHS Employee)

3.7 CCPP Requirements for Customer Relationship Management (CRM)

3.7.1 Facility Requirements

For the net new Netcare facility and existing Netcare facility in the community setting, the following AH privacy and security requirements would need to be met:

1. For the updated expedited Netcare PIA letter the facility will need to have the “new” expedited PIA completed that includes both Netcare and CCPP.
2. The pORA is current to specified timeframe (i.e. eHS current operational standard is within 2 years)

The current onboarding request (OR) process will be updated to add these elements into the Privacy and Security stage of the onboarding request (Ex. The creation of a new Onboarding Request (OR), a new category/subcategory will be created to accommodate for CCPP).

The completion of the PIA and pORA requirements for CCPP would automatically update the CCPP Live status on the main facility page.

3.7.2 User Requirements

The community facility roles are the roles that are captured and stored in the CRM. No eHealth initiative user registration data is currently captured.

The current CRM is on-premise and not connected to source data systems that will be used for the user registration and training requirements steps. Manually updating CCPP end user registration and training data would be an administrative effort to update and maintain ongoing. It seems most efficient for eHS (and other stakeholder teams) to utilize the source systems directly for end user registration, access and training requirement completion data. From that data eHS can provide operational support to mixed context providers and staff.

These below user requirements are proposed to be handled and managed manually for LPR:

1. Epic (Connect Care) Information

Within AHS IAM, through the self-service menu, the mixed context provider and staff submit their personal information into the “Epic (Connect Care) information” questionnaire. The Epic (Connect Care) Information collects the following information:

- Month of Birth
- Date of Birth
- Year of Birth
- Marital Status
- Sex/Gender
- Home Address 1
- Home Address 2
- Home City
- Home Postal Code

2. OOB Training

A CCPP Access Agreement is required to be filled out for each Custodian - eHS will be responsible for ensuring the CCPP Access Agreement has been completed. At this time, the existing CCPP Access Agreement will be used, and electronic signatures will be obtained.

Assumption: The EPIC Access Agreement between AHS and CGI is in place.

3.7.3 Case Management Requirements

Within CRM, to allow cases to be tracked, it has been determined the existing “ANP” Initiative and the existing Categories will be utilized, however new subcategories will be required.

The following is a list of Categories and Subcategories within CRM and the proposed new subcategories are highlighted in green:

Category	Subcategory
User Management	General Inquiry – User Management

	New ANP User
	Request to Audit a Netcare User / Report a Breach
	Require Site User List
	Send / Resend User Credentials
	Update / Reactivate User
	Can't Find or Open Form
	Fax Send / Received Issue
	Reason for Form Rejection
	Require Assistance to Complete Form
	Status of Form / Current Form Processing Timeframe
	180-Day ANP Account Inquiry
	Sunset Date Inquiry
	IMA Inquiry / Status
	Expedite Request
	CCPP–New User
Facility & Custodian Management	Access Administrator Change
	Custodian / Licensee Change
	eHealth Check Inquiry
	General Inquiry – Facility Management
	Ineligible Custodian (ANP)
	Privacy & Security Compliance Support
	New RTI Implementation (PIN/PCR)
	New RTI Implementation (Imm/ARI)
	New ANP Implementation
	New AHS IAM Implementation
	Facility Update / Closure
	CCPP-New Implementation
	CCPP-Privacy and Security Compliance Support
	CCPP-Ineligible Custodian
	CCPP-General Inquiry
Login Issues / Password Reset	Provide ANP Login Assistance
	Provide AHS IAM Login Assistance
	Require ANP Password Reset

	Require AHS IAM Password Reset
	Provide RTI Login Assistance
	Require PIN/PD Password Reset
	CCPP-Provide Login Assistance
Other / Unknown	AHS IAM Other
	ANP Other
	Connect Care Inquiry
	eDelivery Other
	eReferral Other
	HIA Inquiry / Other
	OCME Other
	Other / Unknown
	RTI Other
	CCPP-Other
Remote Access Inquiries (Tokens)	Change Token Type
	Expired / Token Not Working
	Lost / Stolen Token
	Return Token / Token Not Required
	General Token Inquiry
	Token Status
Technical	Other Technical Issue
	AHS IAM Technical Issue
	ANP Technical Issue
	eReferral Technical Issue
	RTI Technical Issue
	Pharmacy Batch Inquiry / Issue
	Citrix Inquiry / Issue
	ANP Data Quality or Integrity Issue
	CCPP-Data Quality or Integrity Issue
	CCPP-Technical Issue
Training and Awareness	Access Administrator Training
	Assist / Redirect AHS Caller
	Community ANP User Training / Functionality Inquiry

	eReferral Training / Functionality Inquiry
	eReferral User / Group Training Request
	AHS ANP User / Group Training Request
	Community ANP User / Group Training Request
	Student Education Training Request
	AHS IAM Training / Functionality Inquiry
	CCPP-User / Group Training Request
	CCPP-Training / Functionality Inquiry

3.8 Support for CCPP User

When a Netcare/CCPP user requires CCPP Support, contact is made to one of the following services:

- eHealth Services Contact Centre
 - By Phone (1-855-643-8649)
 - By Email (eHealthProviderSupport@gov.ab.ca)
- AHS IT Service Desk (Tier 1)
 - By Phone (1-877-311-4300)
- Provincial Service Desk (Tier 1)
 - By Phone (1-877-931-1638)

Where the Netcare/CCPP user is working will determine which support team to call.

- If the Netcare/CCPP user is working at a community facility, the eHealth Services Contact Centre will be contacted.
- If the Netcare/CCPP user is working at an AHS facility, then the AHS IT Service Desk will be contacted.
- If the Netcare/CCPP user needs a Netcare password reset, then the Provincial Service Desk will be contacted.

Note:

All three of these teams work closely together and their top priority is to resolve issues that the Netcare/CCPP user has. If the Netcare/CCPP user contacts the wrong service desk, the Netcare/CCPP user will be redirected to the appropriate team according to the type of issue.

Each team is responsible for certain tasks.

1. eHealth Services Contact Centre

eHS is responsible for handling the following:

- Triage issues accordingly
- Privacy and Security Services Support
- CCPP Training and Registration Services Support

2. AHS IT Service Desk

The AHS IT Service Desk (Tier 1) is responsible for handling the following:

- AHS IAM technical difficulties
- Netcare password reset (Combo role type only)
 - RSA access issues
 - Main line that can triage to the CCPP team, but not to the AHS Bridge team
 - CCPP user has access to CCPP, but cannot log in
 - Technical issue with My Learning Link (MLL) – includes MLL password resets
 - Support by AHS SD + My Learning Link Support line (My Learning Link Support Centre - Hours: M-F 8:30 am to 3:30 pm - 1-888-580-7010)
- MLL Login issues after receiving their MLL (AD) login credentials (possibly due to MFA issues). On the MLL login page external users should be able to utilize the **Update/Change your Password** (if the current password is known) feature, but the **Forgot Your Password?** option is only available if the user is connected to AHS either through RSA, VPN or if at an AHS site. The reason for this is the resource is connected to the IAM system.
- Azure multi-factor authentication

3. Provincial Service Desk

The Provincial Service Desk (Tier 1) is responsible for handling the following:

- Netcare password reset (Community role type only)
- Triage CCPP registration and training questions

For issues that go to the AHS IT Service Team, if they cannot be resolved at the Tier 1 level, the CCPP user will then be redirected to one of the following Tier 2 team within their organization:

- AHS Connect Care Provider Portal IT Team

- AHS Learning Services
- AHS Privacy
- AHS Provider Bridge

AHS Connect Care Provider Portal IT Team is responsible for the following:

- Issues with access to CCPP (i.e. access denied, other login issues, site could not be reached, etc.)
- Help with functionality questions (i.e. can't see In Basket for MOA they are providing coverage for, or the MOA can't see the In Basket for the provider they support)
- Issues accessing information within the patient chart

AHS Learning Services is responsible for the following:

- Course registration
- Course completion errors
- Navigation of the MLL site

MyLearningLink Support

MyLearningLink Support Centre is open Monday to Friday 8:30 – 3:30 pm
1-888-580-7010 or helpmylearninglink@ahs.ca

AHS Privacy is responsible for the following:

- CCPP issues/items that involve breach or potential breach under FOIP or HIA
- Queries or matters that involve authority for access and disclosure to personally identifying personal and health information

AHS Provider Bridge is responsible for the following:

- Receive feedback from users on portal functionality
- Email Address: ccproviderbridge@ahs.ca – this email can be shared external
- This team answers questions that may arise from the community providers such as:
 - What is the difference between Netcare and Connect Care
 - How does the Connect Care Provider Portal support communities?

4 Terms, Acronyms, and Abbreviations

Provide a list of the key terms, acronyms, and abbreviations used in this document.

Term/Acronym	Description
AA	Access Administrator
AD	Active Directory
ADF	Additional Database Fields
AH	Alberta Health
AHS	Alberta Health Services
AHS IAM	Alberta Health Services Identity and Access Management
ANP	Alberta Netcare Portal
CCPP	Connect Care Provider Portal
CRM	Customer Relationship Management
DSR	Delivery Site Registry
HIA	Health Information Act
LPR	Limited Production Rollout
MFA	Multi-Factor Authentication
MLL	My Learning Link
MOU	Memorandum of Understanding
OCME	Office of the Chief Medical Examiner
OOBB	On Our Best Behavior
OR	Onboarding Request
PIA	Privacy Impact Assessment
pORA	Provincial Organizational Readiness Assessment
SAT	Smart Auditing Tool
URF	User Registration Form
WDFA	The 4-digit number that each site receives and is generated by the Delivery Site Registry (DSR)

5 References

Provide a list of the other documents referenced in this document.

File Name and Location	Description
CCPP roles matrix ANP Permission Matrix	ANP Role Permissions Matrix

6 Appendix A: Concept of Operation

Below are the definitions of the specific roles/key terms involved in the onboarding and offboarding process. Depending on the size and make up of a clinic, a single individual may play multiple roles. It is important to understand that each person who accesses CCPP must be identified as a specific role (see table below). The identified ANP roles were used for purposes of developing the CCPP roles, there may be other ANP roles to map to these 3 CCPP roles.

ANP Role		CCPP Role		Difference
Role	Users	Role	Users	Explanation
Clinical 1 & 2	Physicians, Nurse Practitioners	CCPP Clinical 1	Physicians, Nurse Practitioners	<ul style="list-style-type: none"> Roles are equivalent
Clinical 1 & 2	Nurses, Licensed Practical Nurses (LPNs), rarely clinicians in Diagnostic Imaging (DI) clinics	CCPP Clinical 4	Nurses, LPNs	<ul style="list-style-type: none"> CCPP differentiates access required for clinical staff that are governed by a regulated health profession Regulated Healthcare professional (for example, LPN that report to a medical professional association) are accountable to their association CCPP does not include DI clinic staff as this user requires different access. A future role may include this user type
Clinical 1 & 2	Clinical staff, registration staff, HIM, MOA	CCPP Clinical 8	MOA Support (non-regulated professionals): MOA's, general admin	<ul style="list-style-type: none"> CCPP differentiates provider support staff that are not part of a regulated health profession to align with their scope of practice Graduate of a college (non-regulated) providing medical reception training and/or trained by the physician/other staff regarding clinic practices



CCPP via ANP Draft Process Flow and Summary

Ministry

Alberta Health

Division Name:

Health Information Systems

Branch/Unit:

Strategic IMT Services

Creation Date:

September 24, 2024

Print Date:

December 13, 2024

Document Version:

V1.0

Template Location

Primary Contact:	Project Management Office (PMO)	Health.PMO@gov.ab.ca
Template Location:	The master copy of this template is located in the PMO Framework HealthShare Site.	
Template Version	V 1.0.2	
Template Date	May 28, 2014	

Template Usage

This template is being provided by Alberta Health through the PMO, Information Management Branch of Health Information Systems (HIS) Division to provide a common and consistent approach for the delivery of IT-related initiatives and projects.

Some sections of the template may contain *italicized* descriptive information that should be removed once the template has been filled in.

Some projects may require additional elements be added to the deliverable, additional elements may be inserted throughout the document as appropriate. **Note: Removing template sections may introduce risk and potentially affect the success of the project. In the event that a section is not applicable to your project, a brief explanation should be provided as to why it is not applicable.**

Deliverables should wherever possible, be provided in MS Word format. Embedded objects such as diagrams and charts should be created using a common or standard tool such as MS Word and MS Visio and the source objects should be available rather than just a snapshot of the objects.

Your opinion and suggestions for improving this template are important to the PMO, Health Information Systems Division (HIS). The PMO has instituted a review and release process to help improve the templates. Contact the PMO to learn how your input to continuous improvement can be captured.

Table of Contents

DOCUMENT REVISION HISTORY	4
DELIVERABLE APPROVERS AND REVIEWERS	5
1 DOCUMENT PURPOSE.....	7
1.1 BACKGROUND	7
1.2 CURRENT STATE	7
2 PROPOSED SOLUTION	8
3 BUSINESS CONTEXT	9
3.1 BUSINESS DRIVERS	9
3.2 BUSINESS OBJECTIVES	9
4 CCPP VIA ANP DRAFT PROCESS FLOW	10
4.1 EXISTING NETCARE FACILITY – CCPP VIA ANP FOR MIXED CONTEXT PROVIDER AND STAFF	10
4.1.1 Process Flow.....	11
4.1.2 Process Tasks	12
4.2 NET NEW NETCARE FACILITY – CCPP VIA ANP FOR MIXED CONTEXT PROVIDER.....	20
4.2.1 Process Flow.....	21
4.2.2 Process Tasks	22
4.3 CCPP USER OFFBOARDING	30
4.3.1 Process Flow.....	30
4.3.2 Process Tasks	31
4.4 OCME NETCARE/CCPP ONBOARDING	32
4.4.1 Process Flow.....	33
4.4.2 Process Tasks	34
4.5 OCME NETCARE/CCPP USER OFFBOARDING	39
4.5.1 Process Flow.....	40
4.5.2 Process Tasks	40
4.6 SUPPORT FOR CCPP USER DRAFT PROCESS FLOW.....	42
4.6.1 Process Flow.....	43
4.6.2 Process Tasks	43
4.7 CCPP 180-DAY INACTIVE ACCESS ACCOUNT DISABLING	46
4.7.1 Process Flow.....	47
4.7.2 Process Tasks	47
5 SUMMARY OF THE CCPP VIA ANP DRAFT PROCESS FLOWS	50
5.1 EXISTING NETCARE FACILITY – CCPP VIA ANP FOR MIXED CONTEXT PROVIDER AND STAFF.	50
5.2 NET NEW NETCARE FACILITY – CCPP VIA ANP FOR MIXED CONTEXT PROVIDER.....	51
5.3 CCPP USER OFFBOARDING	51
5.4 OCME NETCARE/CCPP ONBOARDING	52
5.5 OCME NETCARE/CCPP USER OFFBOARDING	53
5.6 CCPP SUPPORT DRAFT WORKFLOW	54
5.7 CCPP 180-DAY INACTIVE ACCESS ACCOUNT DISABLING	56
6 TERMS, ACRONYMS, AND ABBREVIATIONS	58
7 REFERENCES	60
8 APPENDIX A – MLL WELCOME EMAIL TEMPLATE.....	61

Document Location**Document Revision History**

Version	Version Date	Summary of Changes	Author
0.1	September 24, 2024	Initial Draft	Lisa Cloutier
0.2	October 29, 2024	Revised based on Business Feedback and more information gained from investigation	Lisa Cloutier
0.3	November 5, 2024	Revised based on feedback from AH and AHS	Lisa Cloutier
0.4	November 15, 2024	Revised based on feedback from AH and AHS	Lisa Cloutier
0.5	November 25, 2024	Revised based on feedback from AH and AHS	Lisa Cloutier
0.6	December 5, 2024	Revised based on feedback from AH and AHS	Lisa Cloutier
0.7	December 6, 2024	Added additional changes to OCME Process Flow and Summary	Lisa Cloutier
0.8	December 10, 2024	Revised based on feedback from AH and AHS	Lisa Cloutier
1.0	December 13, 2024	Final Version	Lisa Cloutier

Deliverable Approvers and Reviewers

Title and Name	Type	Purpose
Todd James Director, Consumer eHealth, AH	A	<i>Reviews and approves</i>
Lisa Brower Director, HIA Policy, Privacy and Security, AH	A	<i>Reviews and approves</i>
Lloyd Thorpe Senior Project Manager, eHealth Ecosystem Modernization, AH	A	<i>Reviews and approves</i>
Ryan Zimmerman Senior Project Manager, Health Information Continuity, Provincial Primary Health Care, AHS	A	<i>Reviews and approves</i>
Stephen Smithbower Director, Health Information Continuity, Provincial Primary Health Care, AHS	A	<i>Reviews and approves</i>
Sharon McNaughton IT Senior Analyst, Ambulatory, EMR and Portals Connect Care, AHS	R	<i>Reviews</i>
Desiree Fadri Senior Consultant, Health Information Continuity, Provincial Primary Health Care, AHS	R	<i>Reviews</i>
Verica Jelic EHR Deployment Manager, AH	A	<i>Reviews and approves</i>

Title and Name	Type	Purpose
Sheri Ross Senior Clinical Specialist, AH	A	<i>Reviews and approves</i>
Amanda Harrigan Policy Advisor HIA, AH	A	<i>Reviews and approves</i>
Rorisang Hlahatsi-Baloyi Senior Management Consultant, Emerging Technology, CGI	R	<i>Reviews</i>
Tara England Director, Consulting Services, eHS Operations Manager, CGI	R	<i>Reviews</i>
Abdul Lawal Director, Consulting Services, eHS Account Manager, CGI	R	<i>Reviews</i>

Type: **A** – Approves (implies review as well); **P** – Prepares; **R** – content review and input; **I** – Information Only

1 Document Purpose

This document outlines the Connect Care Provider Portal (CCPP) via ANP Draft Process flows along with a summary to describe what occurs when a mixed context provider (Lead Custodian) or the Office of the Chief Medical Examiner (OCME) requests access to the CCPP via ANP to help support patient care.

1.1 Background

The Connect Care Provider Portal (CCPP) is a web-based application that allows clinicians and staff (from community sites and OCME) with appropriate role-based access to securely access the health information from Connect Care.

It is designed to improve the continuity of care for patients as they move between sites in AHS and their primary care providers in the community. Clinicians who currently use Alberta Netcare Portal (ANP) will be able to access CCPP via an in-context launch from a tab in ANP.

Previously, AH and AHS collaborated on a project to enable ANP enabled care providers logged in to ANP to launch in context to CCPP (single sign on).

The project was stalled as a result of OIPC feedback regarding the authority identified by AHS for managing the sharing of CCPP patient information to clinicians who are not AHS affiliates.

ADM/Sr. ADMAH direction is to move forward with implementation preparations and deploy to a limited number of users in the Limited Production Rollout (LPR) within the January 2025 timeframe.

1.2 Current State

Currently, providers who work both within AHS and their community clinical practice, referred to as 'mixed context providers' (AHS affiliates), may have Connect Care access through Hyperdrive when working at the AHS site, but when working at the community site these providers, as well as their staff in the community practice, do not and required patient follow up is challenged as a result.

Currently, users in the OCME have Netcare access but do not have CCPP access.

2 Proposed Solution

The Connect Care Provider Portal would allow an Authorized Custodian with ANP access to log into Netcare and to access the CCPP via an in-context launch from a tab in ANP. Once within Connect Care, the user can search for records of other patients.

Deploying CCPP access to providers and their office staff will support the providers and improve both care and informational continuity. To ensure continuity of care and access to required health information, Alberta Health is asserting control over the CCPP. Alberta Health will rely upon authorities that it has as the Ministry of Health under the Health Information Act (HIA) which are not available to AHS.

The primary CCPP project focus is the deployment of CCPP to community providers and their clinic staff with the initial focus on mixed context providers. Leveraging existing Netcare Portal processes for onboarding users, processes will be defined for community providers to request and manage access to the CCPP. Operational processes to support users through the process will also be established.

A secondary project focus is the deployment of CCPP to OCME users with Netcare access. This initiative will involve adapting existing onboarding processes to cater specifically to OCME users, ensuring they can effectively request and manage access to the CCPP system. Operational workflows will be defined to support these users, facilitating a smooth integration of CCPP into their daily practices. Additionally, tailored training and support resources will be established to empower OCME staff, ensuring they are equipped to utilize CCPP effectively in their roles.

In order to allow the sharing of EPIC information between AHS and CGI an EPIC Access Agreement needs to exist. This is in progress, AH is in discussions with HIAPPSU, CGI and AHS - ETA Dec 17/24.

3 Business Context

3.1 Business Drivers

To improve the continuity of care for patients as they move between sites in AHS that use Connect Care and their primary care providers in the community.

To improve access to information required by the OCME to support decision-making and fatality investigations.

3.2 Business Objectives

The objective of this project is to establish processes for granting and managing CCPP via ANP access for mixed context providers (Lead Custodians) and their community clinic staff. This will support continuity of patient care. Additionally, processes will be established for granting and managing CCPP access via ANP for ANP users within the OCME.

4 CCPP via ANP Draft Process Flow

4.1 Existing Netcare Facility – CCPP via ANP For Mixed Context Provider and Staff

The following actors are part of the existing Netcare Facility – CCPP via ANP:

- **Existing Netcare Community Facility**
 - Lead Custodian responsible to request access to CCPP for their staff
 - Netcare Access Administrator (NAA)
 - Mixed Context Providers and Staff
- **eHealth Services Team Resources**
 - Coordinating Agent assigned as a point of contact to Lead Custodian
 - Privacy & Security Services
 - Registration / Forms Services
 - Training (provide training to new NAA or AA refresh training) Services
 - Netcare Contact Centre Support
- **AHS Resources**
 - AHS IAM system
 - AHS CCPP IT Team
 - AHS LDAP

4.1.1 Process Flow

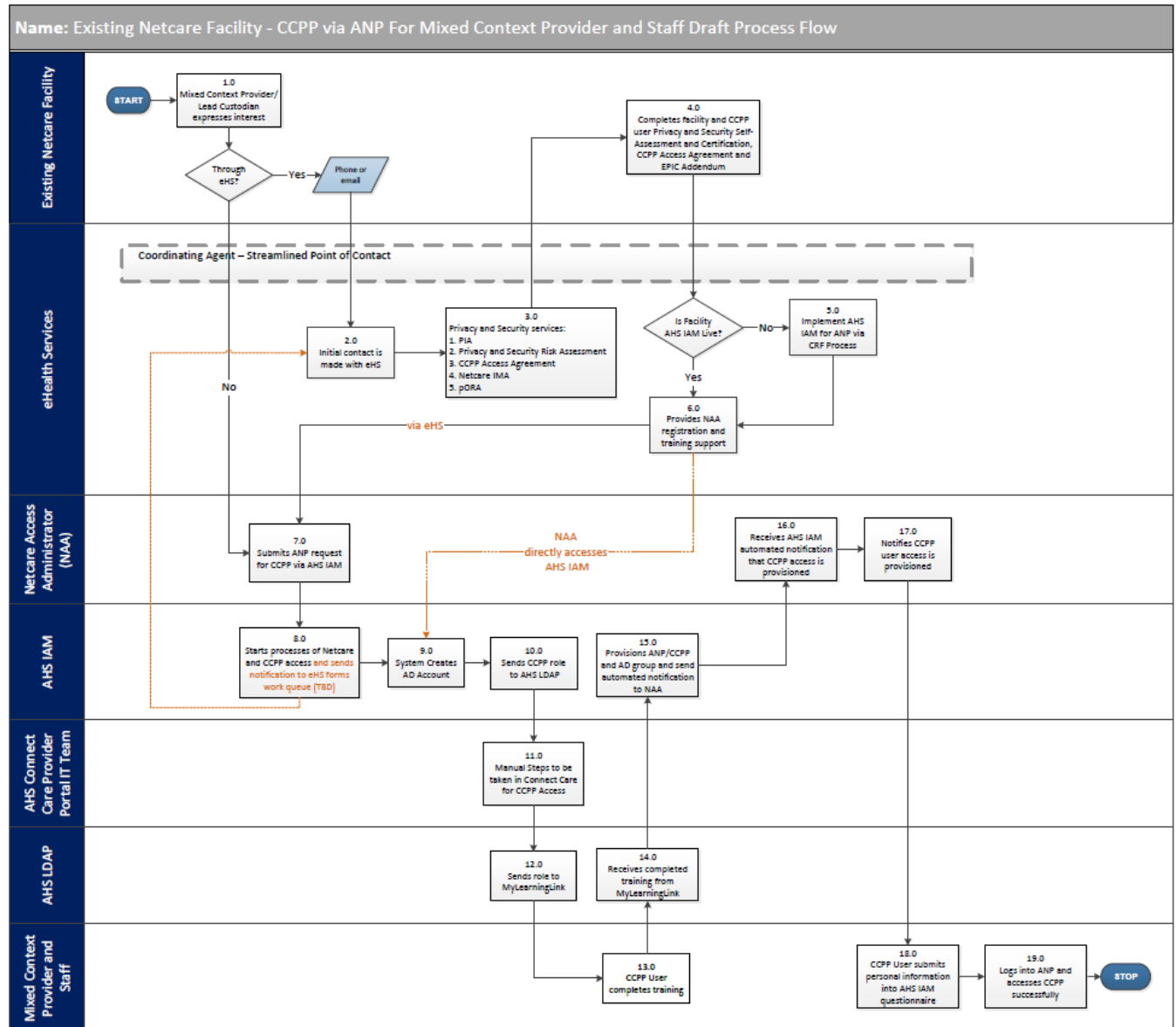


Figure 1 - Existing Netcare Facility - CCPP via ANP for Mixed Context Provider and Staff

4.1.2 Process Tasks

Process Flow Number & Name	Task
1.0 Mixed context provider/Lead Custodian expresses interest	<p>The process begins when the mixed context provider/ Lead Custodian expresses interest for access to CCPP from their community site.</p> <p>For mixed context providers, they will access Connect Care, via Hyperdrive when they are at AHS facilities, but are required to use CCPP via ANP when they are at the community sites. Therefore, CCPP via ANP access will be required for both the mixed context provider (unless already granted) and their community staff.</p>
Indirectly through eHS or directly accessing AHS IAM?	<p>The CCPP request can be initiated one of two ways:</p> <ul style="list-style-type: none"> Through eHS, either by phone or email Through directly accessing AHS IAM <p>If the CCPP request is initiated through eHS then proceed to Step #2.0 Initial contact is made with eHS</p> <p>If the CCPP request is initiated through directly accessing AHS IAM then proceed to Step #7 Submits ANP request for CCPP via AHS IAM</p>
2.0 Initial contact is made through eHS Coordinating Agent (CA) as a point of contact (bundled services offering)	<p>The initial contact is made via inquiry to eHS through the Contact Centre or could be received directly to eHS Service area.</p> <p>With the bundled services approach, there is a new Coordinating Agent role which is the streamlined point of contact between the mixed context provider/Lead Custodian and eHealth services.</p> <p>Therefore, when the Contact Centre/eHS Service area receives a request for CCPP via ANP, the Contact Centre/eHS Service area obtains the required information, then passes this information onto the Coordinating Agent (CA).</p>
3.0 Privacy and Security services: <ul style="list-style-type: none"> PIA Privacy and Security Risk Assessment CCPP Access Agreement Netcare IMA pORA 	<p>The eHS privacy and security services provides support to the mixed context provider (Lead Custodian) to ensure the following:</p> <ul style="list-style-type: none"> PIA Requirements have been met Privacy and Security Risk Assessment has been met CCPP Access Agreement has been signed and submitted Verify Netcare IMA and complete if needed Verify if pORA exists and/or complete a new one if required <p>1. Complete a Privacy Impact (PIA)</p> <p>The following steps are performed:</p> <ul style="list-style-type: none"> Review the Addendum 9 Document Confirm Facility Policies – ensure privacy policies are up-to-date and reflect current systems, practices and privacy and security management

	<ul style="list-style-type: none"> • Complete combined ANP and CCPP via ANP endorsement letter • Submit the combined ANP and CCPP via ANP endorsement letter and the HIA Policies Document to the Information and Privacy Commissioner • Notify eHealth Services team to confirm submission of the PIA and attach a scanned copy of the signed endorsement letter • Confirm PIA Acknowledgement – once the OIPC acknowledgement letter is received, the authorized custodian must email a scanned copy to eHealth Services <p>2. Review and Complete Connect Care Provider Portal Privacy and Security Self-Assessment and Certification</p> <p>The purpose of this Self-Assessment is to provide AH with a certification by the Lead Custodian on behalf of all users at the Clinic that all of them have considered, understood and promoted the privacy and security risk mitigations necessary to access and use the Connect Care Provider Portal (CCPP).</p> <p>The following steps are performed:</p> <ul style="list-style-type: none"> • Obtain the Form - the privacy and security eHealth Consultant will provide a copy of the Self-Assessment form to the authorized custodian or delegated representative • Collaborate with eHealth Consultant - work with the eHealth Consultant to review the Self-Assessment form • The Lead Custodian must complete the Self Assessment, sign the Self-Assessment Certification and then submit the Self-Assessment to eHealthPrivacy@gov.ab.ca on behalf of all Custodians at the clinic. • Once received by eHS, the responses provided for all six sections will be reviewed to ensure the Clinic meets the requirements for access to the CCPP. All questions have to be answered “yes” for the access to be granted to CCPP. • The Self-Assessment will be stored in Sharepoint in a dedicated folder <p>3. Sign CCPP Access Agreement and Epic Addendum</p> <p>Once the custodian’s identity is confirmed, the Lead Custodian and all authorized custodians must sign the CCPP Access Agreement and the Epic Addendum, formalizing their commitment to privacy and security protocols.</p> <p>The following steps are performed:</p> <ul style="list-style-type: none"> • Obtain the Forms - the P&S eHealth Consultant will provide the authorized custodians with a copy of the CCPP Access Agreement and Epic Addendum • Authorized Custodian Signs and Submits the CCPP Access Agreement and Epic Addendum to eHealthPrivacy@gov.ab.ca and eHS enters information into
--	---

	<p>the CCPP Agreement tracker in Sharepoint and uploads the CCPP Access Agreement into Sharepoint</p> <p>Assumption: The EPIC Access Agreement between AHS and CGI is in place.</p> <p>4. Sign an Informational Manager Agreement (IMA) & Review Information Exchange Protocol (IEP) The IMA will only be provided to Authorized Custodian without an IMA on file</p> <ul style="list-style-type: none"> • Obtain the Forms <ul style="list-style-type: none"> ○ The P&S eHealth Consultant will provide the authorized custodian with a copy of an IMA and IEP. • Review the IEP • Sign an IMA <ul style="list-style-type: none"> ○ Learn more about the IMA by reading the IMA/IEP factsheet. <p>5. If required, Review and Complete a new Provincial Organization Readiness Assessment (pORA)</p> <p>The pORA is a critical security assessment for community facilities seeking access to Alberta Netcare applications. The pORA evaluates administrative, physical, and technical security standards and ensures that the facility can protect personal health information.</p> <p>The following steps are performed:</p> <ul style="list-style-type: none"> • Obtain the Form - the privacy and security eHealth Consultant will provide a copy of the assessment form (pORA) to the authorized custodian or delegated representative • Collaborate with eHealth Consultant - work with the eHealth Consultant to review an existing pORA or complete a new pORA form. • Submit pORA - if a new pORA is required, the eHealth Consultant will submit it to the Alberta Health HIA Policy, Privacy, and Security Unit for review and approval • Meet All Security Standards - once Alberta Health confirms the responses meet security standards, the authorized custodian will sign the pORA <p>Timeline: The review and approval process for the pORA can take several weeks, depending on the facility's specific circumstances.</p> <p>Validity Period: The pORA remains valid for two years, after which it must be updated to ensure continued compliance with security standards.</p> <p>Interim State: Security Self-Assessment needs to be completed by Lead Custodian on behalf of all Custodian of the clinic</p> <p>Note: As part of eHealth Support when speaking to the Lead</p>
--	--

	Custodian, it is very important to ensure each user has a valid personal email address. Although personal email address is not mandatory, is vital for the CCPP process. If a valid personal email address is not provided, then the user will not be able to access MLL.
4.0 Completes facility and CCPP user Privacy and Security Self-Assessment and Certification, CCPP Access Agreement and Epic Addendum	The mixed context provider or Lead Custodian completes the privacy and security requirements that is provided by eHS as detailed above.
Is Facility AHS IAM Live? (Decision Point)	Being AHS IAM Live means that the facility has been setup within AHS IAM so that the NAA can manage (add and/or remove) access for Custodians at the facility site. eHS CA checks Is facility in AHS IAM Live? If facility is not AHS IAM Live, then proceed to Step #5.0 Implement AHS IAM for ANP via Custodian Registration Form (CRF) Process If facility is AHS IAM Live, then proceed to Step #6 Provide NAA registration and training support
5.0 Implement AHS IAM for ANP via CRF Processes	eHS will support the facility with the CRF process. As part of completing the CRF process, the eHS Forms Management Services will add WDFA to the ANP Rollout List in AHS IAM and send out the AHS IAM Username to the NAA Role(s)
6.0 Provides NAA registration and training support	eHS CA provides the following: <ul style="list-style-type: none"> • NAA registration and training support <ul style="list-style-type: none"> ○ Roles and Responsibilities ○ AHS IAM Training (functionality) <p>If initial contact was made through eHS proceed to 7.0 Submits ANP request for CCPP via AHS IAM.</p> <p>If the NAA already has access to AHS IAM then eHS will offer AA refresher training and proceed to 9.0 System creates AD Account (this is represented by the dashed orange line in the diagram going from box 6.0 Provides NAA registration and training support to box 9.0 System creates AD Account)</p>
7.0 Submits ANP request for CCPP via AHS IAM	Community facilities using AHS IAM for ANP can submit ANP request with CCPP optional access with or without engaging with eHS before this step. Within AHS IAM, when requesting access, the display of the CCPP access checkbox is configurable so that it will not appear on the screen until it has been turned on. Being configurable will allow the CCPP access to be turned on without a code release. Once the ability to request CCPP access is put into place it will be available to all facilities (may not be restricted by facility), but there will be mechanisms put in place so the requestors that see the CCPP access checkbox will have the ANP role of Clinical 1 or Clinical 2

	<p>only. Therefore, professions such as Pharmacists will not see the CCPP access checkbox.</p> <p>The NAA goes into AHS IAM and submits an ANP request for CCPP access for the mixed context provider and the community site staff.</p> <p>Note: A Custodian may work at multiple facilities, having the same or different roles at each facility and if this is the case the Netcare AA at each facility should submit a request for CCPP access within AHS IAM if CCPP access is required at each facility. At the present time, CCPP access is not WDFA specific therefore when a Custodian receives CCPP access, the Custodian is able to view the information for all facilities they are associated with. Even though the Custodian must select the facility from a dropdown list when accessing ANP, CCPP does not limit the Custodian to viewing only the information specific to the selected WDFA. This could be an enhancement in the future but at this time CCPP access is not WDFA specific. Also, if the Custodian has different roles at different facilities then the role with the higher level of privileges will be provided to the Custodian for all facilities they are associated with. This detail has been added to the risk log.</p>
<p>8.0 Starts processes of Netcare and CCPP access and sends notification to eHS forms work queue</p>	<p>Currently, Community sites using AHS IAM for ANP get automated email notifications indicating the request has been submitted and work queue item is sent directly to the NAA role, who has requested the access.</p> <p>An automated email notification will also be sent to an eHS shared mailbox (eHealthPrivacy@gov.ab.ca) so in cases where the NAA goes directly into AHS IAM, without going through eHS, steps can be built to support eHS review of PIA and pORA to ensure all privacy and security requirements have been met as well as ensure the CCPP Access Agreement has been completed for each Custodian at the community site.</p> <p>For the LPR phase, if a requestor that is not part of the LPR requests CCPP access for themselves and/or their staff, there needs to be appropriate controls in place as part of the Onboarding process to prevent CCPP access to be granted. An email notification needs to be sent to eHS and then eHS will reach out to the requestor to inform that this clinic is not part of the LPR and CCPP access cannot be granted at this time. Need to ensure that CCPP access is only granted to the appropriate people.</p>
<p>9.0 System Creates AD account</p>	<p>AHS IAM automates the creation of the Active Directory account via a connector with Active Directory.</p> <p>The sub-category and company selected on the Network Activation Request (NAR) drives the Organizational Unit (OU) that the account is created in.</p> <p>There is a Community User OU that these accounts will be created in.</p>
<p>10.0 Sends CCPP role to AHS LDAP</p>	<p>Roles map to templates which map to training in MyLearningLink (MLL).</p>

	<p>AHS IAM sends the template name to AHS LDAP via connector (as well as a number of other data points that are important to MyLearningLink (MLL)).</p> <p>This template is then set to scheduled as a signal to the system that the user has been registered for training but has not yet completed the training.</p> <p>A work item (an email notification) is created within AHS IAM and sent to the AHS CCPP IT Team to determine if requestor should receive CCPP access (has to have an ANP role of Clinical 1 or Clinical 2 and be part of LPR).</p> <p>As part of the EPIC workflow when a CCPP role is assigned and approved, the user and NAA will receive an automated email from the AHS IAM system indicating a role has been assigned to the user, outlines the associated training required and contains the MLL link to allow access to the training.</p>
11.0 Manual Steps to be taken in Netcare for CCPP Access	<p>The Connect Care Provider IT Team:</p> <ul style="list-style-type: none"> • Receives notification that the CCPP role has been assigned • Adds User Context to EMP Managed Access setting.
12.0 Sends role to MyLearningLink	<p>Both OOBB and the ECL 200 Introduction to CCPP are existing e-learning courses within MLL.</p> <p>AHS LDAP has an API with MLL.</p> <p>This API sends updated information to MLL every 15 minutes with users that have recently been registered for roles.</p> <p>Once MLL receives this information a user is able to register for training.</p> <p>The information that MLL receives from AHS LDAP is what sets the level of access that an end-user will have in MLL and what training they will be able to access.</p> <p>As soon as a user has been given access to MLL (given a profile within MLL by AHS IAM), if the user has not previously accessed MLL, an automated "Welcome" email notification will be sent to the user from the MLL system that indicates access has been granted. This email provides the user information about how to access the MLL system. This Welcome email is configurable so an AHS Communication person from Learning Services will work with others to design the email and include the correct wording.</p> <p>If the user has already previously accessed MLL then an automated Welcome email notification will not be sent out to the user because the user is already within the MLL system.</p> <p>The publishing of the MLL will be through the Unified Access Portal (UAP- public facing portal) using the user's existing RSA soft token – this has been successfully tested and confirmed to be technically viable within MLL Production the UAP test environment.</p> <p>AHS has confirmed that a custom training email can be sent out to the end user instead of a form one.</p>

13.0 CCPP User completes training	The CCPP User completes the required OOB and ECL 200 Introduction to CCPP training
14.0 Receives completed training from MyLearningLink	<p>Configuration can be setup to determine what roles access and complete what mandatory courses.</p> <p>Once a provider has completed the mandatory training, the training does not have to be taken again within a 3-year timeframe. Training records are kept, and the Welcome email will not be sent to them within the 3 years.</p> <p>Note: It is a requirement that the mandatory training be taken once again after a 3-year period, but currently there is nothing in place to enforce this and CCPP access is not disabled when the 3-year period is up. At this time there is no automated email sent out to the user to indicate that the training needs to be taken again. This will be revisited at a later date and Ryan will add this to the parking lot for future enhancement. AHS has indicated that reports can be run to determine which users need to take the mandatory training over due to the time lapse being over 3 years.</p> <p>AHS LDAP is notified from MyLearningLink (MLL) the training has been completed by the CCPP user.</p> <p>Tableau queries MLL every 4 hours and pulls back all training results.</p> <p>The MLLTrainingTrack field in AHS LDAP is then directly updated to completed (when training is completed).</p> <p>That completed status is pushed to AHS IAM.</p> <p>When it is detected AHS IAM provisions access for the template/role that was associated.</p> <p>Once the role is provisioned AHS IAM changes the status of the role in AHS LDAP to provisioned (alternate statuses are cancelled, revoked, and retrain).</p>
15.0 Provisions ANP/CCPP and AD group and sends automated notification to NAA	<p>AHS IAM automates the provisioning of Epic accounts; there is an API that creates the actual account and assigns the template to the end-user.</p> <p>A work item will be generated for the Connect Care Provider IT Team.</p> <p>Automated notifications are sent out to the NAA.</p>
16.0 Receives AHS IAM automated notification that CCPP access is provisioned	<p>The NAA receives an automated notification from the AHS IAM system that CCPP access is provisioned for the mixed context provider and staff. This automated notification also includes instructions on how to complete the Epic (Connect Care) Information questionnaire (Smart Audit Tool).</p> <p>If the Epic Information has not been completed within 15 days from the date the email was sent, a reminder email like the first one will be sent to the requestor and the Netcare Authorized Approver(s).</p> <p>An additional 15 days will be provided to complete the Epic</p>

	<p>Information in AHS IAM.</p> <p>After an additional 15 days, if the Epic Information is still not completed, the Epic (Connect Care) access will be blocked. To unblock your access, enter your Epic Information in IAM.</p>
17.0 Notifies CCPP user access is provisioned	The NAA notifies the mixed context provider and staff their CCPP access has been provisioned and provides instructions on how to access and complete the Epic (Connect Care) information questionnaire (Smart Audit Tool).
18.0 CCPP User submits personal information into AHS IAM questionnaire	<p>Within AHS IAM, through the self-service menu, the mixed context provider and staff submit their personal information into the "Epic (Connect Care) information" questionnaire (Smart Audit Tool).</p> <p>Instructions to complete your Epic (Connect Care) Information (Smart Audit Tool)</p> <ul style="list-style-type: none"> - LAUNCH the AHS Identity & Access Management (IAM) system - If you are accessing IAM remotely, you will be prompted to enter an RSA SecurID token passcode. If you do not have an RSA SecurID token, go to an AHS site to access IAM. - LOGIN using your AHS Network UserID and Password OR your IAM Username and Password - CLICK on Self Service in that pane or in the menu bar - CLICK on Epic (Connect Care) Information (Smart Audit Tool) - ENTER the required information - CLICK Save - LOGOUT of IAM <p>The information required is as follows:</p> <ul style="list-style-type: none"> • Month of Birth • Date of Birth • Year of Birth • Marital Status, • Sex/Gender • Home Address 1 • Home Address 2 • Home City • Home Postal Code <p>Once entered, the information can be modified at any time.</p>
19.0 Logs into ANP and accesses CCPP successfully	<p>The provider and/or affiliate(s) receive notification that access is ready, logs into Alberta Netcare Portal and launches CCPP successfully.</p> <p>Within ANP the button to access CCPP reads as "CC Provider Portal". At the present time there is a change request to have the name of the button within ANP changed from "CC Provider Portal" to "CCPP", but this change will not be implemented until March 2025 at the earliest.</p>

	Note: Once the user is registered for CCPP optional access at one WDFA if they have multiple community WDFA's they will be able to access the CC Provider Portal tab across any facility. WDFA is not being passed at this time but is a future consideration: to be put into place in about 6 months to a year timeframe.
--	--

4.2 Net New Netcare Facility – CCPP via ANP for Mixed Context Provider

The following actors are part of the net new Netcare Facility – CCPP via ANP:

- **Net New Netcare Community Facility**
 - Lead Custodian responsible to request access to CCPP for their staff
 - Netcare Access Administrator (NAA)
 - Mixed Context Providers and Staff
- **eHealth Services Team Resources**
 - Coordinating Agent assigned as a point of contact to Lead Custodian
 - Facilities DSR / Management Services
 - Privacy & Security Services
 - Registration / Forms Services
 - Training (provide training to new NAA or AA refresh training)
 - Netcare Contact Centre Support
- **AHS Resources**
 - AHS IAM system
 - AHS CCPP IT Team
 - AHS LDAP

4.2.1 Process Flow

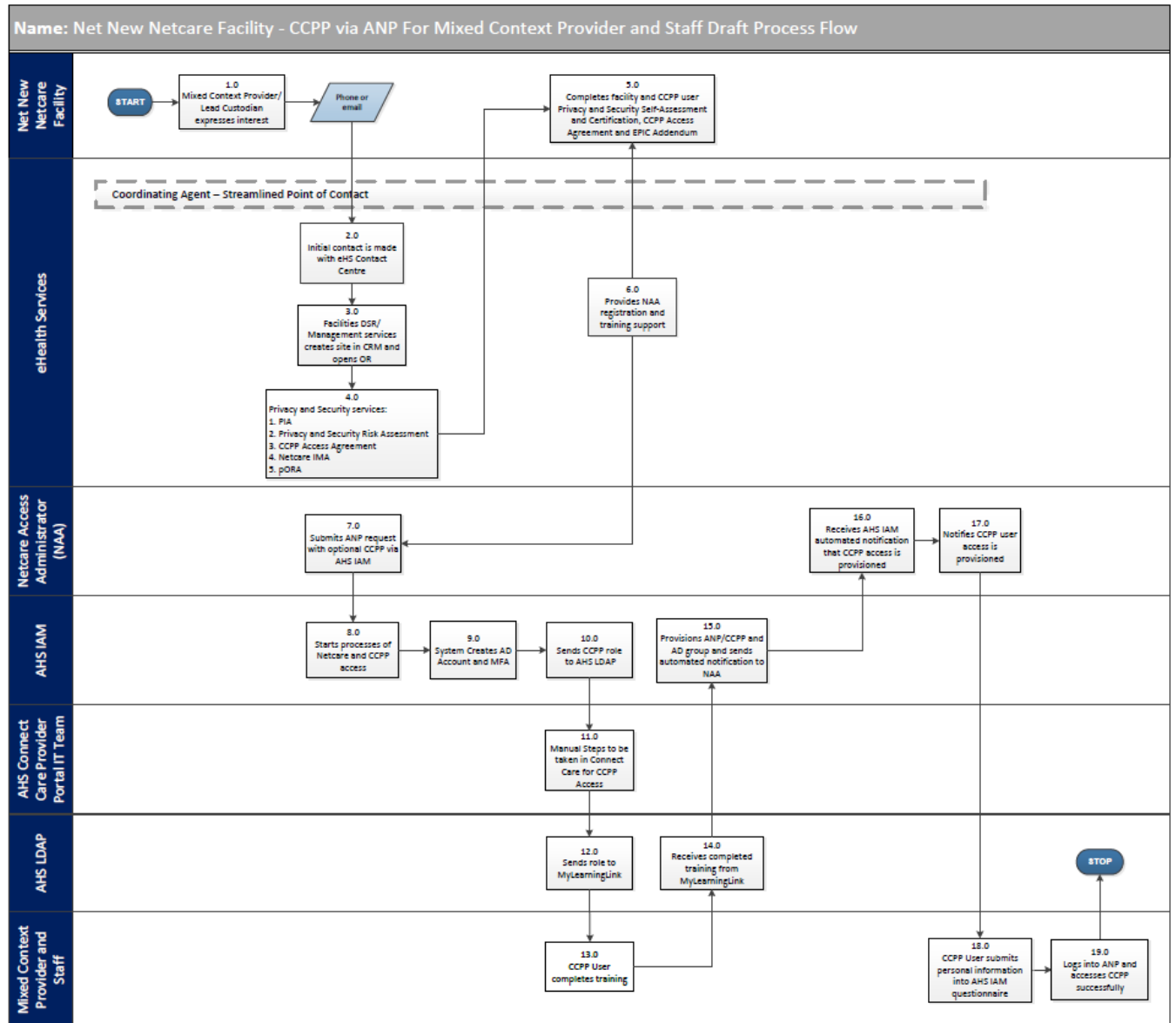


Figure 2 - Net New Netcare Facility - CCPP via ANP for Mixed Context Provider and Staff

4.2.2 Process Tasks

Process Flow Number & Name	Task
1.0 Mixed Context Provider/Lead Custodian expresses interest	<p>The process begins when the mixed context provider/Lead Custodian expresses interest either by phone or email requesting Netcare and optional CCPP access for themselves and/or the community clinic staff.</p> <p>For mixed context providers, they will access Connect Care, via Hyperdrive when they are at AHS facilities, but are required to use CCPP via ANP when they are at the community sites. Therefore, CCPP via ANP access will be required for both the context mixed provider (unless already granted) and their community staff.</p>
2.0 Initial contact is made with the eHS Contact Centre Coordinating Agent (CA) as a point of contact (bundled services offering)	<p>The initial contact is made via inquiry to the eHS Contact Centre.</p> <p>With the bundled services approach, there is a new Coordinating Agent role which is the streamlined point of contact between the mixed context provider (Lead Custodian) and eHealth services.</p> <p>Therefore, when the eHS Contact Centre receives a request for Netcare and optional CCPP via ANP, the Contact Centre obtains the required information, then passes this information onto the Coordinating Agent (CA).</p>
3.0 Facilities DSR/Management services create site in CRM	<p>The eHS Facility DSR/Management services receives DSR Notification of new WDFA and creates the site in CRM so the onboarding process can be initiated.</p> <p>The eHS Facility DSR/Management services initiates the onboarding process by creating the Onboarding Request (OR) in CRM.</p> <p>This step will be completed by the Coordinating Agent if the facility site already exists within CRM.</p> <p>Coordinating Agent (CA) Intake and Facility Registration</p> <p>Once initial contact has been made, the following steps are performed:</p> <ul style="list-style-type: none"> • Verify eligibility of the requestor as an authorized custodian through professional college websites • Confirm and update contact information via DSR, CRM, IMA SS and ANP systems • Review registration requirements and process details with the clinic • Send a personalized email outlining the next steps in the onboarding process • Update CRM with all relevant information • Agree on follow-up dates for further assistance
4.0 Privacy and Security services: <ul style="list-style-type: none"> • PIA • Privacy and Security Risk Assessment • CCPP Access Agreement 	<p>The eHS privacy and security services provides support to the mixed context provider (Lead Custodian) to ensure the following:</p> <ul style="list-style-type: none"> • PIA Requirements have been met • Privacy and Security Risk Assessment has been met

<ul style="list-style-type: none"> • Netcare IMA • pORA 	<ul style="list-style-type: none"> • CCPP Access Agreement has been signed and submitted • Verify Netcare IMA and complete if needed • Verify if pORA exists and/or complete a new one if required <p>1. Complete a Privacy Impact (PIA)</p> <p>The following steps are performed:</p> <ul style="list-style-type: none"> • Review the Addendum 9 Document • Confirm Facility Policies – ensure privacy policies are up-to-date and reflect current systems, practices and privacy and security management • Complete combined ANP and CCPP via ANP endorsement letter • Submit the combined ANP and CCPP via ANP endorsement letter and the HIA Policies Document to the Information and Privacy Commissioner • Notify eHealth Services team to confirm submission of the PIA and attach a scanned copy of the signed endorsement letter • Confirm PIA Acknowledgement – once the OIPC acknowledgement letter is received, the authorized custodian must email a scanned copy to eHealth Services <p>2. Review and Complete Connect Care Provider Portal Privacy and Security Self-Assessment and Certification</p> <p>The purpose of this Self-Assessment is to provide AH with a certification by the Lead Custodian on behalf of all users at the Clinic that all of them have considered, understood and promoted the privacy and security risk mitigations necessary to access and use the Connect Care Provider Portal (CCPP).</p> <p>The following steps are performed:</p> <ul style="list-style-type: none"> • Obtain the Form - the privacy and security eHealth Consultant will provide a copy of the Self-Assessment form to the authorized custodian or delegated representative • Collaborate with eHealth Consultant - work with the eHealth Consultant to review the Self-Assessment form • The Lead Custodian must complete the Self Assessment, sign the Self-Assessment Certification and then submit the Self-Assessment to eHealthPrivacy@gov.ab.ca on behalf of all Custodians at the clinic. • Once received by eHS, the responses provided for all six sections will be reviewed to ensure the Clinic meets the requirements for access to the CCPP. All questions have to be answered “yes” for the access to be granted to CCPP. • The Self-Assessment will be stored in Sharepoint in a dedicated folder <p>3. Sign CCPP Access Agreement and Epic Addendum</p>
---	--

	<p>Once the custodian's identity is confirmed, the Lead Custodian and all authorized custodians must sign the CCPP Access Agreement and the Epic Addendum, formalizing their commitment to privacy and security protocols.</p> <p>The following steps are performed:</p> <ul style="list-style-type: none"> • Obtain the Forms - the P&S eHealth Consultant will provide the authorized custodians with a copy of the CCPP Access Agreement and Epic Addendum • Authorized Custodian Signs and Submits the CCPP Access Agreement and Epic Addendum to eHealthPrivacy@gov.ab.ca and eHS enters information into the CCPP Agreement tracker in Sharepoint and uploads the CCPP Access Agreement into Sharepoint <p>Assumption: The EPIC Access Agreement between AHS and CGI is in place.</p> <p>4. Sign an Informational Manager Agreement (IMA) & Review Information Exchange Protocol (IEP) The IMA will only be provided to Authorized Custodian without an IMA on file</p> <ul style="list-style-type: none"> • Obtain the Forms <ul style="list-style-type: none"> ◦ The P&S eHealth Consultant will provide the authorized custodian with a copy of an IMA and IEP. • Review the IEP • Sign an IMA <ul style="list-style-type: none"> ◦ Learn more about the IMA by reading the IMA/IEP factsheet. <p>5. Complete a new Provincial Organization Readiness Assessment (pORA)</p> <p>The pORA is a critical security assessment for community facilities seeking access to Alberta Netcare applications. The pORA evaluates administrative, physical, and technical security standards and ensures that the facility can protect personal health information.</p> <p>The following steps are performed:</p> <ul style="list-style-type: none"> • Obtain the Form - the privacy and security eHealth Consultant will provide a copy of the assessment form (pORA) to the authorized custodian or delegated representative • Collaborate with eHealth Consultant - work with the eHealth Consultant to review an existing pORA or complete a new pORA form. • Submit pORA - if a new pORA is required, the eHealth Consultant will submit it to the Alberta Health HIA Policy, Privacy, and Security Unit for review and approval • Meet All Security Standards - once Alberta Health confirms the responses meet security standards, the authorized custodian will sign the pORA
--	--

	<p>Timeline: The review and approval process for the pORA can take several weeks, depending on the facility's specific circumstances.</p> <p>Validity Period: The pORA remains valid for two years, after which it must be updated to ensure continued compliance with security standards.</p> <p>Interim State: Security Self-Assessment needs to be completed by Lead Custodian on behalf of all Custodian of the clinic</p> <p>Note: As part of eHealth Support when speaking to the Lead Custodian, it is very important to ensure each user has a valid personal email address. Although personal email address is not mandatory, is vital for the CCPP process. If a valid personal email address is not provided, then the user will not be able to access MLL.</p>
5.0 Completes facility and CCPP user privacy/security Self-Assessment and Certification and CCPP Access Agreement and Epic Addendum	The mixed context provider or Lead Custodian completes the privacy and security requirements that is provided by eHS as detailed above.
6.0 Provides NAA registration and training support	<p>eHS provides the following:</p> <ul style="list-style-type: none"> NAA registration and training support <ul style="list-style-type: none"> Roles and Responsibilities AHS IAM Training (functionality)
7.0 Submits ANP request with optional CCPP via AHS IAM	<p>Within AHS IAM, when requesting access, the display of the CCPP access checkbox is configurable so that it will not appear on the screen until it has been turned on. Being configurable will allow the CCPP access to be turned on without a code release.</p> <p>Once the ability to request CCPP access is put into place it will be available to all facilities (may not be restricted by facility), but there will be mechanisms put in place so the requestors that see the CCPP access checkbox will have the ANP role of Clinical 1 and Clinical 2 only. Therefore, professions such as Pharmacists will not see the CCPP access checkbox.</p> <p>The NAA goes into AHS IAM and submits an ANP request with optional CCPP access for the mixed context provider and the community site staff.</p> <p>Note: A Custodian may work at multiple facilities, having the same or different roles at each facility and if this is the case the Netcare AA at each facility should submit a request for CCPP access within AHS IAM if CCPP access is required at each facility. At the present time, CCPP access is not WDFA specific therefore when a Custodian receives CCPP access, the Custodian is able to view the information for all facilities they are associated with. Even though the Custodian must select the facility from a dropdown list when accessing ANP, CCPP does not limit the Custodian to viewing only the information</p>

	<p>specific to the selected WDFA. This could be an enhancement in the future but at this time CCPP access is not WDFA specific. Also, if the Custodian has different roles at different facilities, then the role with the higher level of privileges will be provided to the Custodian for all facilities they are associated with. This detail has been added to the risk log.</p>
<p>8.0 Starts processes of Netcare and CCPP access</p>	<p>Currently, Community sites using AHS IAM for ANP get automated email notifications indicating the request has been submitted and work queue item is sent directly to the NAA role, who has requested the access.</p> <p>An automated email notification will also be sent to an eHS shared mailbox (eHealthPrivacy@gov.ab.ca) so in cases where the NAA goes directly into AHS IAM, without going through eHS, steps can be built to support eHS review of PIA and pORA to ensure all privacy and security requirements have been met as well as ensure the CCPP Access Agreement has been completed for each Custodian at the community site.</p> <p>The ANP access process is already well document, will proceed as normal, and will run separately from the CCPP access much like Remote User Network Access (RUNA) does today. If the CCPP access request is stalled for any reason, this will not affect the ANP access, the ANP access will proceed as normal.</p> <p>For the LPR phase, if a requestor that is not part of the LPR requests CCPP access for themselves and/or their staff, there needs to be appropriate controls in place as part of the Onboarding process to prevent CCPP access to be granted. An email notification needs to be sent to eHS and then eHS will reach out to the requestor to inform that this clinic is not part of the LPR and CCPP access cannot be granted at this time. Need to ensure that CCPP access is only granted to the appropriate people.</p>
<p>9.0 System Creates AD account</p>	<p>AHS IAM automates the creation of the Active Directory account via a connector with Active Directory.</p> <p>The sub-category and company selected on the Network Activation Request (NAR) drives the Organizational Unit (OU) that the account is created in.</p> <p>There is a Community User OU that these accounts will be created in.</p>
<p>10.0 Sends CCPP role to AHS LDAP</p>	<p>Roles map to templates which map to training in MLL.</p> <p>AHS IAM sends the template name to AHS LDAP via connector (as well as a number of other data points that are important to MyLearningLink (MLL)).</p> <p>This template is then set to scheduled as a signal to the system that the user has been registered for training but has not yet completed the training.</p> <p>A work item (an email notification) is created within AHS IAM and sent to the AHS CCPP IT Team to determine if requestor should</p>

	<p>receive CCPP access (has to have an ANP role of Clinical 1 or Clinical 2 and be part of LPR).</p> <p>As part of the EPIC workflow when a CCPP role is assigned and approved, the user and NAA will receive an automated email from the AHS IAM system indicating a role has been assigned to the user, outlines the associated training required and contains the MLL link to allow access to the training.</p>
<p>11.0</p> <p>Manual Steps to be taken in Netcare for CCPP Access</p>	<p>The Connect Care Provider IT Team:</p> <ul style="list-style-type: none"> • Receives notification that the CCPP role has been assigned • Adds User Context to EMP Managed Access setting
<p>12.0</p> <p>Sends role to MyLearningLink</p>	<p>Both OOBB and the ECL 200 Introduction to CCPP are existing e-learning courses within MLL.</p> <p>AHS LDAP has an API with MLL.</p> <p>This API sends updated information to MLL every 15 minutes with users that have recently been registered for roles.</p> <p>Once MLL receives this information a user is able to register for training.</p> <p>The information that MLL receives from AHS LDAP is what sets the level of access that an end-user will have in MLL and what training they will be able to access.</p> <p>As soon as a user has been given access to MLL (given a profile within MLL by AHS IAM), if the user has not previously accessed MLL, an automated "Welcome" email notification will be sent to the user from the MLL system that indicates access has been granted. This email provides the user information about how to access the MLL system. This Welcome email is configurable so an AHS Communication person from Learning Services will work with others to design the email and include the correct wording.</p> <p>If the user has already previously accessed MLL then an automated Welcome email notification will not be sent out to the user because the user is already within the MLL system.</p> <p>The publishing of the MLL will be through the Unified Access Portal (UAP- public facing portal) using the user's existing RSA soft token – this has been successfully tested and confirmed to be technically viable within MLL Production the UAP test environment.</p> <p>AHS confirmed that a custom training email can be sent out to the end user instead of a form one.</p>
<p>13.0</p> <p>CCPP User completes training</p>	<p>The CCPP User completes the required OOBB and ECL 200 Introduction to CCPP training</p>
<p>14.0</p> <p>Receives completed training from MyLearningLink</p>	<p>Configuration can be setup to determine what roles access and complete what mandatory courses.</p> <p>Once a provider has completed the mandatory training, the training does not have to be taken again within a 3-year timeframe. Training records are kept, and the Welcome email will not be sent to them</p>

	<p>within the 3 years.</p> <p>Note: It is a requirement that the mandatory training be taken once again after a 3-year period, but currently there is nothing in place to enforce this and CCPP access is not disabled when the 3-year period is up. At this time there is no automatic email sent out to the user to indicate that the training needs to be taken again. This will be revisited at a later date and Ryan will add this to the parking lot for future enhancement. AHS has indicated that reports can be run to determine which users need to take the mandatory training over due to the time lapse being over 3 years.</p> <p>AHS LDAP is notified from MyLearningLink the training has been completed by the CCPP user.</p> <p>Tableau queries MLL every 4 hours and pulls back all training results. The MLLTrainingTrack field in AHS LDAP is then directly updated to completed (when training is completed).</p> <p>That completed status is pushed to AHS IAM.</p> <p>When it is detected AHS IAM provisions access for the template/role that was associated.</p> <p>Once the role is provisioned AHS IAM changes the status of the role in AHS LDAP to provisioned (alternate statuses are cancelled, revoked, and retrain).</p>
15.0 Provisions ANP/CCPP and AD group and sends automated notification to NAA	<p>AHS IAM automates the provisioning of Epic accounts; there is an API that creates the actual account and assigns the template to the end-user.</p> <p>A work item will be generated for the Connect Care Provider IT Team.</p> <p>Automated notifications are sent out to the NAA.</p>
16.0 Receives AHS IAM automated notification that CCPP access is provisioned	<p>The NAA receives an automated notification from the AHS IAM system that CCPP access is provisioned for the mixed context provider and staff. This automated notification also includes instructions on how to access and complete the Epic (Connect Care) Information questionnaire (Smart Audit Tool).</p> <p>If the Epic Information has not been completed within 15 days from the date the email was sent, a reminder email like the first one will be sent to the requestor and the Netcare Authorized Approver(s).</p> <p>An additional 15 days will be provided to complete the Epic Information in AHS IAM.</p> <p>After an additional 15 days, if the Epic Information is still not completed, the Epic (Connect Care) access will be blocked. To unblock your access, enter your Epic Information in IAM.</p>
17.0 Notifies CCPP user access is provisioned	<p>The NAA notifies the mixed context provider and staff their CCPP access has been provisioned and provides instructions on how to access and complete the Epic (Connect Care) information questionnaire (Smart Audit Tool).</p>

<p>18.0</p> <p>CCPP User submits personal information into AHS IAM questionnaire</p>	<p>Within AHS IAM, through the self-service menu, the mixed context provider and staff submits their personal information into the “Epic (Connect Care) information” questionnaire (Smart Audit Tool).</p> <p>Instructions to complete your Epic (Connect Care) Information (Smart Audit Tool)</p> <ul style="list-style-type: none"> - LAUNCH the AHS Identity & Access Management (IAM) system - If you are accessing IAM remotely, you will be prompted to enter an RSA SecurID token passcode. If you do not have an RSA SecurID token, go to an AHS site to access IAM. - LOGIN using your AHS Network UserID and Password OR your IAM Username and Password - CLICK on Self Service in that pane or in the menu bar - CLICK on Epic (Connect Care) Information - ENTER the required information - CLICK Save - LOGOUT of IAM <p>The information required is as follows:</p> <ul style="list-style-type: none"> • Month of Birth • Date of Birth • Year of Birth • Marital Status, • Sex/Gender • Home Address 1 • Home Address 2 • Home City • Home Postal Code <p>Once entered, the information can be modified at any time.</p>
<p>19.0</p> <p>Logs into ANP and accesses CCPP successfully</p>	<p>The provider and/or affiliate(s) receive notification that access is ready, logs into Alberta Netcare Portal and launches CCPP successfully.</p> <p>Within ANP the button to access CCPP reads as “CC Provider Portal”. At the present time there is a change request to have the name of the button within ANP changed from “CC Provider Portal” to “CCPP”, but this change will not be implemented until March 2025 at the earliest.</p> <p>Note:</p> <p>Once the user is registered for CCPP optional access at one WDFA if they have multiple community WDFA’s they will be able to access the CC Provider Portal tab across any facility. WDFA is not being passed at this time but is a future consideration: to be put into place in about 6 months to a year timeframe.</p>

4.3 CCPP User Offboarding

The following actors are part of the CCPP User Offboarding – CCPP via ANP:

- **Existing Netcare Community Facility**
 - Mixed Context Provider / Lead Custodian responsible to request removal of access to CCPP for their staff
 - Netcare Access Administrator (NAA)
- **eHealth Services Team Resources**
 - Coordinating Agent assigned as a point of contact to Lead Custodian
 - Netcare Contact Centre Support
- **AHS Resources**
 - AHS IAM system
 - AHS CCPP Team

4.3.1 Process Flow

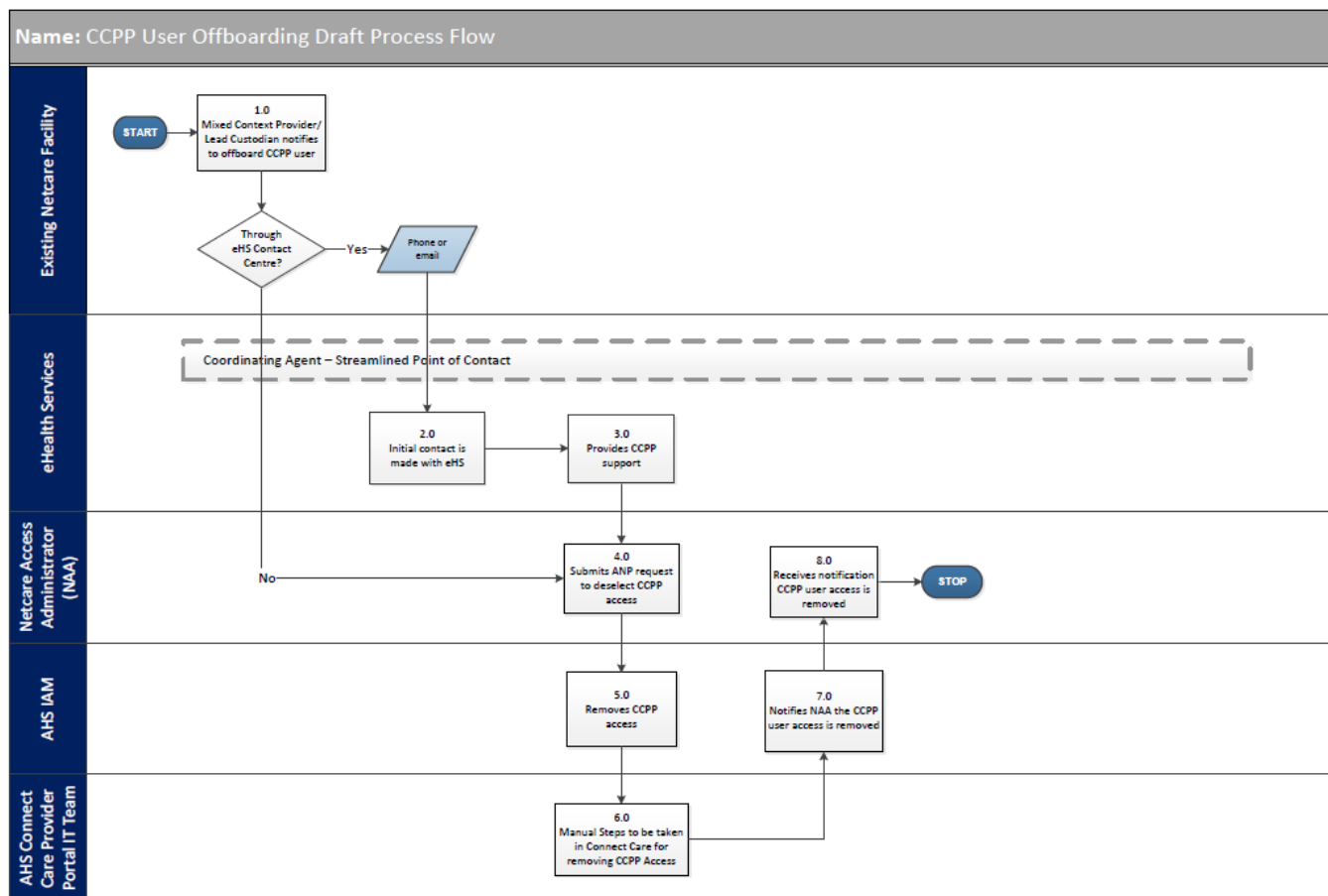


Figure 3 - CCPP User Offboarding

4.3.2 Process Tasks

Process Flow Number & Name	Task
1.0 Mixed Context Provider/Lead Custodian notifies to offboard CCPP user	<p>The process begins when the mixed context provider or Lead Custodian of the existing Netcare facility notifies to offboard the CCPP user.</p> <p>This can be initiated one of the following ways:</p> <ul style="list-style-type: none"> • Contacting eHS Contact Centre either by phone or email • Submitting a request through AHS IAM
Through eHS Contact Centre? (Decision Point)	<p>If the mixed context provider or Lead Custodian of the existing Netcare facility notifies to offboard through the Contact Centre, then proceed to Step #2.0 Initial contact is made with eHS.</p> <p>If the mixed context provider or Lead Custodian of the existing Netcare facility notifies to offboard directly through AHS IAM, then proceed to Step #4 Submits ANP request to deselect CCPP access</p>
2.0 Initial contact is made with eHS	<p>The initial contact is made via inquiry to the Contact Centre.</p> <p>With the bundled services approach, there is a new Coordinating Agent role which is the streamlined point of contact between the mixed context provider or Lead Custodian and eHealth services therefore when the Contact Centre receives a request to remove CCPP via ANP access, the Contact Centre obtains the required information, then passes this information onto the Coordinating Agent.</p> <p>This step will be skipped if the requestor goes directly into AHS IAM to request the removal of CCPP access.</p>
3.0 Provides CCPP support	<p>eHS Services provides CCPP support.</p> <p>This step will be skipped if the requestor goes directly into AHS IAM to request the removal of CCPP access.</p>
4.0 Submits ANP request to deselect CCPP access	<p>The Netcare Access Administrator (NAA) submits an ANP request to deselect CCPP access in AHS IAM</p>
5.0 Removes CCPP access	<p>The ANP request to remove CCPP access for the specified custodian is processed.</p> <p>Note: A Custodian may be registered for CCPP access at multiple facilities. Therefore, if a request is created to remove CCPP access at one facility, the CCPP access will be removed for the specified facility only. The CCPP request for other facilities that the Custodian may still have will remain unless there is other request(s) to remove CCPP access for each facility.</p> <p>This is an automated process within AHS IAM. There is a direct API with Epic which will remove the template for CCPP and inactivates the account (if it is the last template).</p>

	<p>The connector with Active Directory will also remove the CCPP AD group.</p> <p>A work item will be generated for the Connect Care Provider Portal IT Team.</p> <p>Note: The user will not have access to MLL when their CCPP access (from the last associated facility) has been removed.</p>
6.0 Manual Steps to be taken in Netcare for removing CCPP access	<p>The Connect Care Provider IT Team:</p> <ul style="list-style-type: none"> Removes CCPP User Context from end user EMP If the CCPP user is a prescriber: <ul style="list-style-type: none"> Remove from the Provider Group
7.0 Notifies NAA the CCPP user access is removed	<p>The AHS IAM system sends an automated notification to the NAA informing of the removal of the CCPP Access for the specified custodian</p>
8.0 Receives notification CCPP user access is removed	<p>The NAA receives an automated notification from the AHS IAM system that CCPP access has been removed for the specified custodian</p>

4.4 OCME Netcare/CCPP Onboarding

The following actors are part of the OCME Netcare/CCPP Onboarding – CCPP via ANP:

- **OCME**
 - OCME responsible to request access to CCPP for their staff
 - OCME Users
- **eHealth Services Team Resources**
 - eHS Privacy and Security Services
 - Netcare Contact Centre Support
- **HIAPPSU**
 - HIAPPSU (Director and Team)
 - HIAPPSU Access Administrator (AA)
- **AHS Resources**
 - AHS Medical Affairs
 - AHS IAM system
 - AHS CCPP Team
 - AHS LDAP

4.4.1 Process Flow

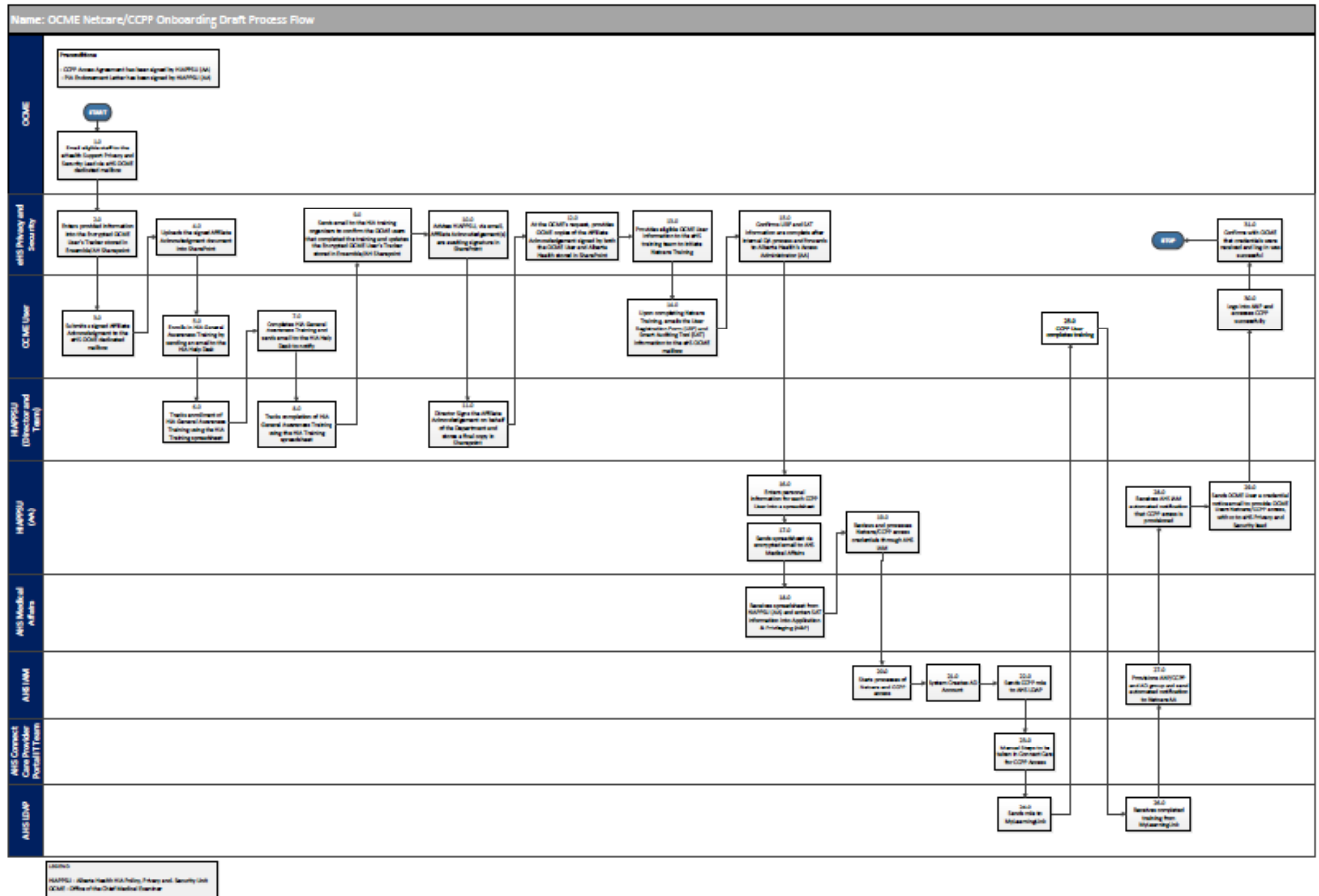


Figure 4 - OCME Netcare/CCPP Onboarding

4.4.2 Process Tasks

Process Flow Number & Name	Task
1.0 Email eligible staff to the eHealth Support Privacy and Security Lead via eHS OCME dedicated mailbox	<p>The OCME provides, to the eHealth Support Privacy and Security lead, a list of OCME staff who meet the eligibility criteria to become OCME Users.</p> <p>The OCME liaison is responsible for determining OCME User eligibility.</p> <p>An email must be sent to the eHS OCME dedicated mailbox (CA.SM.PRJ.eHealth.OCME@cgi.com) the email must include the OCME staff member's name, job role, regulated health profession, and office location (Edmonton or Calgary) for each new requested OCME User.</p> <p>Note: If User already has Netcare access through AHS they must be provisioned access via AH to use for their role with the OCME.</p>
2.0 Enters provided information into the Encrypted OCME User's Tracker stored in Ensemble/AH Sharepoint	The eHS Privacy and Security lead enters this information into the Encrypted OCME User Tracker stored in Ensemble/AH Sharepoint.
3.0 Submits a signed Affiliate Acknowledgement to the eHS OCME dedicated mailbox	<p>Each OCME User must provide a signed Affiliate Acknowledgment document (all FOUR pages).</p> <p>OCME User sends signed Affiliate Acknowledgement documents to the eHS OCME dedicated mailbox.</p>
4.0 Uploads the signed Affiliate Acknowledgement document into Sharepoint	The eHS Privacy and Security lead uploads the signed Affiliate Acknowledgment document into SharePoint.
5.0 Enrolls in HIA General Awareness Training by sending an email to the HIA Help Desk	The OCME User must enroll in HIA General Awareness Training held on the third Wednesday of each month by sending an email to the HIA Help Desk (hiahelpdesk@gov.ab.ca) and cc to eHS OCME dedicated mailbox (eHealthOCM@cgi.com)
6.0 Tracks enrollment of HIA General Awareness Training using the HIA Training spreadsheet	HIAPPSU (Director and Team) tracks OCME User's enrollment in the HIA General Awareness Training and enters information in the HIA Training spreadsheet by Alberta Health.
7.0 Completes HIA General Awareness Training and sends email to the HIA Help Desk to notify	The OCME User completes the HIA General Awareness Training and sends an email to the HIA Help Desk to notify to training has been completed.
8.0	HIAPPSU (Director and Team) tracks OCME Users completion of

Tracks completion of HIA General Awareness Training using the HIA Training spreadsheet	HIA General Awareness Training and enters information in the HIA Training spreadsheet by Alberta Health.
9.0 Sends email to the HIA training organizers to confirm the OCME users that completed the training and updates the Encrypted OCME User's Tracker stored in Ensemble/AH Sharepoint	The eHS Privacy and Security lead will send an email to the HIA training organizers to confirm the list of the OCME users that completed the training and then will add the users to the Encrypted OCME User Tracker stored in Ensemble by eHS Privacy and Security lead.
10.0 Advises HIAPPSU, via email, Affiliate Acknowledgement(s) are awaiting signature in Sharepoint	The eHS Privacy and Security lead will advise the Director, HIAPPSU via email that the Affiliate Acknowledgement are awaiting signature in SharePoint.
11.0 Director signs the Affiliate Acknowledgement on behalf of the Department and stores a final copy in Sharepoint	The Director, HIAPPSU will sign the Affiliate Acknowledgement on behalf of the Department and will store a final copy in SharePoint.
12.0 At the OCME's request, provides OCME copies of the Affiliate Acknowledgement signed by both the OCME User and Alberta Health stored in Sharepoint	The eHS Privacy and Security lead will update the Encrypted OCME User's Tracker stored in Ensemble. At the OCME's request, the eHS Privacy and Security lead will provide OCME copies of the Affiliate Acknowledgement signed by both the OCME User and Alberta Health stored in SharePoint.
13.0 Provides eligible OCME User information to the eHS training team to initiate Netcare Training	Once HIA General Awareness Training is complete, and the Affiliate Acknowledgement has been signed, the eHS Privacy and Security lead will provide the eligible OCME User information to the eHS training team to begin the process of providing Netcare Training to the OCME Users. The eHS Privacy and Security lead will inform the eHS Training Services lead that new OCME users are ready for training with preference to have a training session dedicated to a group of OCME users only and offer the option to join a regular training session for the rest of the OCME users unable to join the dedicated session.
14.0 Upon completing Netcare Training, emails the User Registration Form (URF) and Smart Auditing Tool (SAT) Information to the eHS OCME mailbox	OCME User completes Netcare Training. When an OCME User's Netcare training has been completed, they will email the User Registration Form (URF) and the Smart Auditing Tool (SAT) information to the dedicated eHS OCME mailbox. Recommendation: The current URF does not collect all the SAT information required therefore a new customized URF form will need to be created specifically for OCME to include the additional information as listed above or another separate smaller form

	(template) to collect the above information
15.0 Confirms URF and SAT information are complete after internal review QA process and forwards it to Alberta Health's Access Administrator (AA)	eHS Privacy and Security lead will confirm that the URF and SAT information are complete after internal QA process, will ensure that HIA training and affiliate acknowledgement is complete on the Encrypted OCME User's Tracker stored in Ensemble, and will forward it to Alberta Health's Access Administrator (AA) who will review and process through AHS IAM.
16.0 Enters SAT information for each CCPP User into a spreadsheet	<p>The Netcare Access Administrator (AA) enters the following SAT information from each CCPP user into a spreadsheet:</p> <ul style="list-style-type: none"> • Month of Birth • Date of Birth • Year of Birth • Marital Status, • Sex/Gender • Home Address 1 • Home Address 2 • Home City • Home Postal Code
17.0 Sends spreadsheet via encrypted email to AHS Medical Affairs	Once all CCPP users for the facility are entered on the spreadsheet then the Netcare AA sends the spreadsheet via encrypted email to AHS Medical Affairs
18.0 Receives spreadsheet from Netcare AA and enters CCPP User information into Application & Privileging (A&P)	AHS Medical Affairs receives the spreadsheet and enters the information into Application & Privileging (A&P). Once the information is entered, A&P sends the information to AHS LDAP.
19.0 Reviews and processes Netcare/CCPP access credentials through AHS IAM	Netcare AA reviews and processes the Netcare/CCPP access credentials through AHS IAM.
20.0 Starts processes of Netcare and CCPP access	<p>The ANP access process is already well document, will proceed as normal, and will run separately from the CCPP access much like Remote User Network Access (RUNA) does today. If the CCPP access request is stalled for any reason, this will not affect the ANP access, it will proceed as normal.</p> <p>Currently, a work queue item is sent directly to the HIAPPSU role, who has requested the CCPP access.</p> <p>For the LPR phase, if HIAPPSU requests CCPP access for an OCME site that is not part of the LPR, there needs to be appropriate controls in place as part of the Onboarding process to prevent CCPP access to be granted. An email notification needs to be sent to eHS and then eHS will reach out to the HIAPPSU to inform that this OCME is not part of the LPR and CCPP access cannot be granted at this time. Need to ensure that CCPP access is only granted to the appropriate</p>

	people.
21.0 System Creates AD account	<p>AHS IAM automates the creation of the Active Directory account via a connector with Active Directory.</p> <p>The sub-category and company selected on the Network Activation Request (NAR) drives the Organizational Unit (OU) that the account is created in.</p> <p>There is a Community User OU that these accounts will be created in.</p>
22.0 Sends CCPP role to AHS LDAP	<p>Roles map to templates which map to training in MLL.</p> <p>AHS IAM sends the template name to AHS LDAP via connector (as well as a number of other data points that are important to MLL).</p> <p>This template is then set to scheduled as a signal to the system that the user has been registered for training but has not yet completed the training.</p> <p>A work item (an email notification) is created within AHS IAM and sent to the AHS CCPP IT Team to determine if requestor should receive CCPP access (has to have an ANP role of Clinical 1 or Clinical 2 and be part of LPR).</p> <p>As part of the EPIC workflow when a CCPP role is assigned and approved, the user and NAA will receive an automated email from the AHS IAM system indicating a role has been assigned to the user, outlines the associated training required and contains the MLL link to allow access to the training.</p>
23.0 Manual Steps to be taken in Netcare for CCPP Access	<p>The Connect Care Provider IT Team:</p> <ul style="list-style-type: none"> • Receives notification that the CCPP role has been assigned • Adds User Context to EMP Managed Access setting
24.0 Sends role to MyLearningLink	<p>Both On Our Best Behavior (OOBB) and the ECL 200 Introduction to CCPP are existing e-learning courses within MLL.</p> <p>AHS LDAP has an API with MLL.</p> <p>This API sends updated information to MLL every 15 minutes with users that have recently been registered for roles.</p> <p>Once MLL receives this information a user is able to register for training.</p> <p>The information that MLL receives from AHS LDAP is what sets the level of access that an end-user will have in MLL and what training they will be able to access.</p> <p>As soon as a user has been given access to MLL (given a profile within MLL by AHS IAM), if the user has not previously accessed MLL, an automated "Welcome" email notification will be sent to the user from the MLL system that indicates access has been granted. This email provides the user information about how to access the MLL system. This Welcome email is configurable so an AHS Communication person from Learning Services will work with others</p>

	<p>to design the email and include the correct wording.</p> <p>If the user has already previously accessed MLL then an automated Welcome email notification will not be sent out to the user because the user is already within the MLL system.</p> <p>The publishing of the MLL will be through the Unified Access Portal (UAP- public facing portal) using the user's existing RSA soft token – this has been successfully tested and confirmed to be technically viable within MLL Production the UAP test environment.</p> <p>AHS confirmed that a custom training email can be sent out to the end user instead of a form one.</p>
25.0 CCPP User completes training	The CCPP User completes the required OOB and ECL 200 Introduction to CCPP training
26.0 Receives completed training from MyLearningLink	<p>Configuration can be setup to determine what roles access and complete what mandatory courses.</p> <p>Once a provider has completed the mandatory training, the training does not have to be taken again within a 3-year timeframe. Training records are kept, and the Welcome email will not be sent to them within the 3 years.</p> <p>Note: It is a requirement that the mandatory training be taken once again after a 3-year period, but currently there is nothing in place to enforce this and CCPP access is not disabled when the 3-year period is up. At this time there is no automatic email sent out to the user to indicate that the training needs to be taken again. This will be revisited at a later date and Ryan will add this to the parking lot for future enhancement. AHS has indicated that reports can be run to determine which users need to take the mandatory training over due to the time lapse being over 3 years.</p> <p>AHS LDAP is notified from MyLearningLink the training has been completed by the CCPP user.</p> <p>Tableau queries MLL every 4 hours and pulls back all training results.</p> <p>The MLLTrainingTrack field in AHS LDAP is then directly updated to completed (when training is completed).</p> <p>That completed status is pushed to AHS IAM.</p> <p>When it is detected AHS IAM provisions access for the template/role that was associated.</p> <p>Once the role is provisioned AHS IAM changes the status of the role in AHS LDAP to provisioned (alternate statuses are cancelled, revoked, and retrain).</p>
27.0 Provisions ANP/CCPP and AD group and sends automated notification to Netcare AA	<p>AHS IAM automates the provisioning of Epic accounts; there is an API that creates the actual account and assigns the template to the end-user.</p> <p>A work item will be generated for the Connect Care Provider IT Team.</p> <p>Automated notifications are sent out to the Netcare Access</p>

	Administrator (AA).
28.0 Receives AHS IAM automated notification that CCPP access is provisioned	<p>The HIAPPSU (AA) receives an automated notification from the AHS IAM system that CCPP access is provisioned for the mixed context provider and staff. This automated notification also includes instructions on how to complete the Epic (Connect Care) Information questionnaire (Smart Audit Tool).</p> <p>If the Epic Information has not been completed within 15 days from the date the email was sent, a reminder email like the first one will be sent to the requestor and the Netcare Authorized Approver(s).</p> <p>An additional 15 days will be provided to complete the Epic Information in AHS IAM.</p> <p>After an additional 15 days, if the Epic Information is still not completed, the Epic (Connect Care) access will be blocked. To unblock your access, enter your Epic Information in IAM.</p>
29.0 Sends OCME User a credential notice email to provide OCME Users Netcare/CCPP access, with cc to eHS Privacy and Security Lead	Once access is complete the HIAPPSU Access Administrator (AA) will send the OCME User a credential notice email to provide OCME Users Netcare/CCPP access, with cc to eHS Privacy and Security lead.
30.0 Logs into ANP and accesses CCPP successfully	<p>The OCME user logs into ANP and accesses CCPP successfully.</p> <p>Within ANP the button to access CCPP reads as "CC Provider Portal". At the present time there is a change request to have the name of the button within ANP changed from "CC Provider Portal" to "CCPP", but this change will not be implemented until March 2025 at the earliest.</p>
31.0 Confirms with OCME that credentials were received and log-in was successful	eHS Privacy and Security confirms with OCME that credentials were received by the CCPP user(s) and successful log-in to CCPP via ANP was achieved successfully

4.5 OCME Netcare/CCPP User Offboarding

The following actors are part of the OCME Netcare/CCPP User Offboarding – CCPP via ANP:

- **OCME**
 - OCME responsible to request removal of the access to CCPP for their staff
 - Netcare Access Administrator (NAA)
- **eHealth Services Team Resources**
 - eHS Privacy and Security Services
- **Alberta Health**

- Access Administrator responsible for submitting ANP request to remove access to CCPP for their staff
- **AHS Resources**
 - AHS IAM system
 - AHS CCPP Team

4.5.1 Process Flow

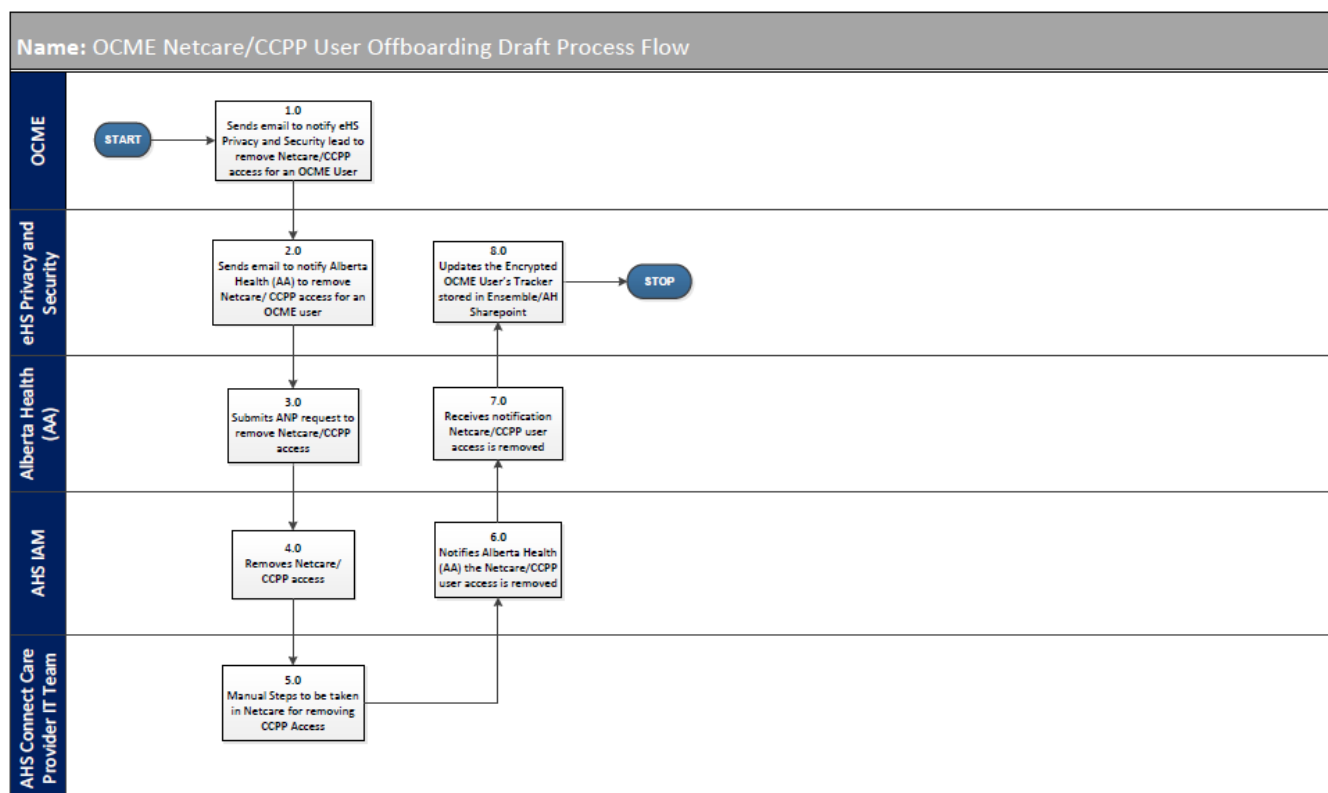


Figure 5 - OCME Netcare/CCPP User Offboarding

4.5.2 Process Tasks

Process Flow Number & Name	Task
1.0 Sends email to notify eHS Privacy and Security lead to remove Netcare/CCPP access for an OCME User	The OCME must notify eHS Privacy and Security lead immediately if any OCME User ceases to be employed or contracted by the OCME. OCME must send an email to the eHS Privacy and Security lead, and the email should include a descriptive subject line, the name of the OCME User and the date the OCME User ceases to be employed or contracted by the OCME.
2.0 Sends email to notify Alberta	eHS Privacy and Security lead notifies Alberta Health (AA) to

Health (AA) to remove Netcare/CCPP access for an OCME user	terminate OCME user's Netcare/CCPP access via email.
3.0 Submit ANP request to remove Netcare/CCPP access	The Alberta Health (AA) submits an ANP request to remove Netcare/CCPP access in AHS IAM
4.0 Removes Netcare/CCPP access	<p>The ANP request to remove CCPP access for the specified custodian is processed.</p> <p>Note: A Custodian may be registered for CCPP access at multiple facilities. Therefore, if a request is created to remove CCPP access at one facility, the CCPP access will be removed for the specified facility only. The CCPP request for other facilities that the Custodian may still have will remain unless there is other request(s) to remove CCPP access for each facility.</p> <p>This is an automated process within AHS IAM. There is a direct API with Epic which will remove the template for CCPP and inactivates the account (if it is the last template).</p> <p>The connector with Active Directory will also remove the CCPP AD group.</p> <p>A work item will be generated for the Connect Care Provider IT Team.</p> <p>Note: The user will not have access to MLL when their CCPP access (from the last associated facility) has been removed.</p>
5.0 Manual Steps to be taken in Netcare for removing CCPP Access	<p>The Connect Care Provider IT Team:</p> <ul style="list-style-type: none"> • Removes CCPP User Context from the end user EMP • If the CCPP user is a prescriber: <ul style="list-style-type: none"> ○ Remove from the Provider Group
6.0 Notifies Alberta Health (AA) the Netcare/CCPP user access is removed	The AHS IAM system sends an automated notification to the Alberta Health (AA) informing of the removal of the Netcare/CCPP access for the specified custodian
7.0 Receives notification Netcare/CCPP user access is removed	The Alberta Health (AA) receives an automated notification from the AHS IAM system that Netcare/CCPP access has been removed for the specified custodian
8.0 Updates the Encrypted OCME User's Tracker stored in Ensemble/AH Sharepoint	The eHS Privacy and Security lead will update the Encrypted OCME User's Tracker stored in Ensemble to indicate that the user access was deleted.

4.6 Support for CCPP User Draft Process Flow

The following actors are part of the Support for CCPP Users – CCPP via ANP:

- **CCPP User**
 - CCPP User that requires CCPP Support
- **eHealth Services Team Resources**
 - eHS Provider Contact Centre
- **AHS Resources**
 - AHS IT Service Desk
 - AHS CCPP IT Team
 - AHS Learning Services
 - AHS Privacy
 - AHS Provider Bridge
- **AH Resources**
 - Provincial Service Desk

4.6.1 Process Flow

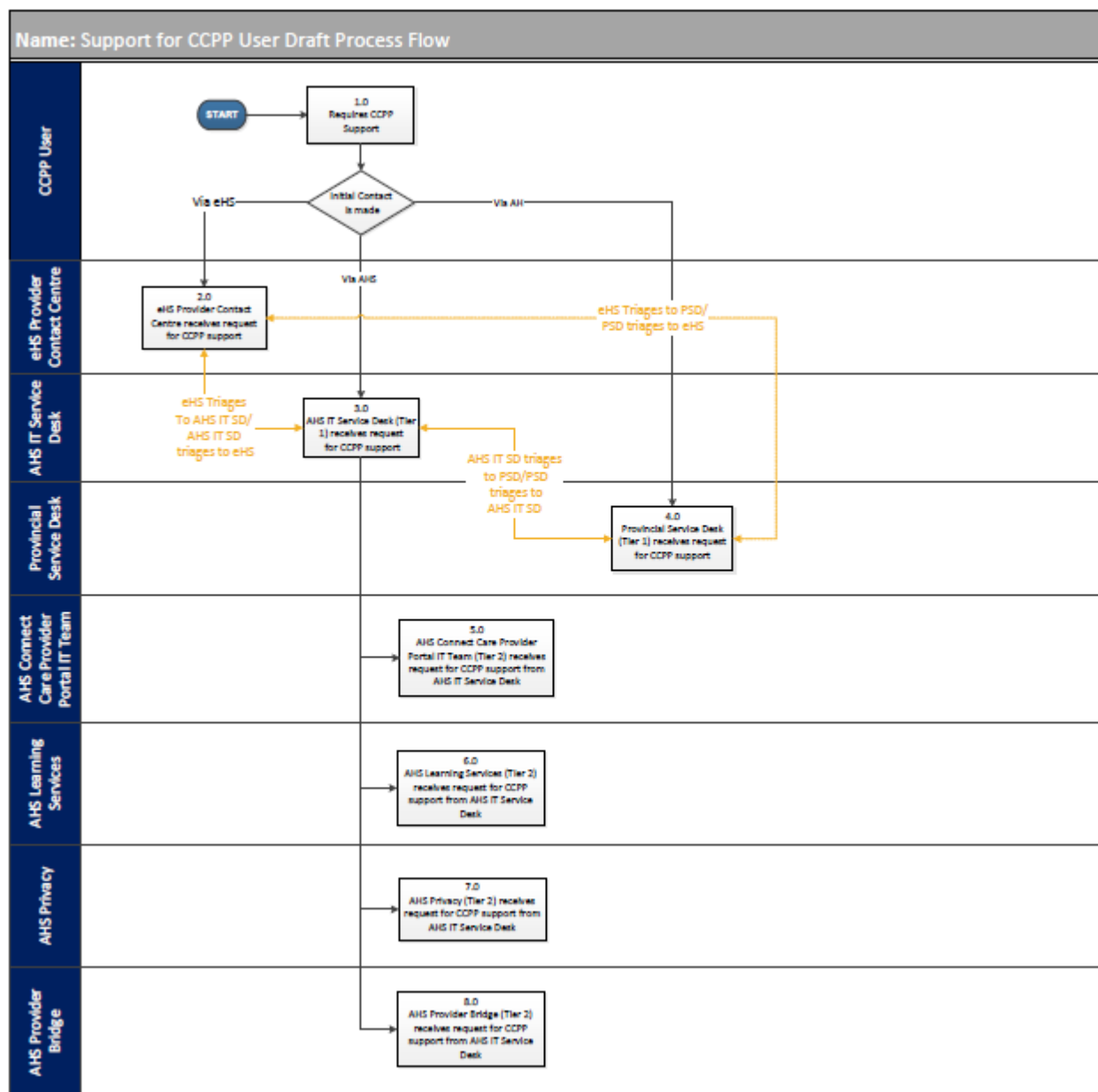


Figure 6- Support for CCPP User

4.6.2 Process Tasks

Process Flow Number & Name	Task
1.0 Requires CCPP Support	CCPP User has as issue and needs support

Initial Contact is made	<p>When a CCPP user needs CCPP Support, contact is made with one of the following:</p> <ul style="list-style-type: none"> eHealth Services <ul style="list-style-type: none"> Phone (1-855-643-8649) Email (eHealthProviderSupport@gov.ab.ca) AHS IT Service Desk <ul style="list-style-type: none"> Phone (1-877-311-4300) Provincial Service Desk <ul style="list-style-type: none"> Phone (1-877-931-1638) <p>If contact was made via eHS Services, then proceed to Step #2.0 eHS Provider Contact Centre receives request for CCPP support.</p> <p>If contact was made via AHS, then proceed to Step #3.0 AHS IT Service Desk (Tier 1) receives request for CCPP support.</p> <p>If contact was made via AH, then proceed to Step #4.0 Provincial Service Desk (Tier 1) receives request for CCPP support.</p>
2.0 eHS Provider Contact Centre receives request for CCPP support	<p>eHS Provider Contact Centre receives a request for CCPP support.</p> <p>eHS Provider Contact Centre provides supports for issues such as:</p> <ul style="list-style-type: none"> Triaging issues accordingly Privacy and Security Services Support CCPP Training and Registration Services Support <p>Note:</p> <p>If eHS determines the issue is out of their realm and should be handled by either AHS IT Service Desk or the Provincial Service Desk, eHS will direct the CCPP user to the appropriate team.</p>
3.0 AHS IT Service Desk (Tier 1) receives request for CCPP support	<p>AHS IT Service Desk receives a request for CCPP support.</p> <p>The AHS IT Service Desk (Tier 1) provides support for issues such as:</p> <p>Tier 1:</p> <ul style="list-style-type: none"> AHS IAM Technical Difficulties <ul style="list-style-type: none"> Support by AHS SD + IAM Team (Chanin) Netcare Password Reset (for Combo role type only) RSA access issues Main line that can triage to the CCPP team, but not to the AHS Bridge team CCPP user has access to CCPP, but cannot log in Technical issue with MLL – includes MLL password resets <ul style="list-style-type: none"> Support by AHS SD + MyLearningLink Support line (MyLearningLink Support Centre - Hours: M-F 8:30 am to 3:30 pm - 1-888-580-7010) MLL Login issues after receiving their MLL (AD) login credentials (possibly due to MFA issues). On the MLL login page external users should be able to utilize the

	<p>Update/Change your Password (if the current password is known) feature, but the Forgot Your Password? option is only available if the user is connected to AHS either through RSA, VPN or if at an AHS site. The reason for this is the resource is connected to the IAM system.</p> <ul style="list-style-type: none"> Azure multi-factor authentication <p>Note:</p> <p>If AHS IT Service Desk determines the issue is out of their realm and should be handled by either eHS or the Provincial Service Desk, AHS IT Service Desk will direct the CCPP user to the appropriate team.</p>
4.0 Provincial Service Desk (Tier 1) receives request for CCPP support	<p>The Provincial Service Desk (Tier 1) receives a request for CCPP support.</p> <p>The Provincial Service Desk (Tier 1) provides support for issues such as:</p> <ul style="list-style-type: none"> Netcare Password Reset (for Community role type only) Triage CCPP Registration and Training Questions <p>Note:</p> <p>If Provincial Service Desk determines the issue is out of their realm and should be handled by either eHS or AHS IT Service Desk, Provincial Service Desk will direct the CCPP user to the appropriate team.</p>
5.0 AHS Connect Care Provider Portal IT Team (Tier 2) receives request for CCPP support from AHS IT Service Desk	<p>AHS Connect Care Provider IT Team (Tier 2) receives a request for CCPP support from the AHS IT Service Desk.</p> <p>The AHS Connect Care Provider IT Team (Tier 2) provides support for issues such as:</p> <ul style="list-style-type: none"> Issues with access to CCPP (i.e. access denied, other login issues, site could not be reached, etc.) Help with functionality questions e.g. can't see In Basket for MOA they are providing coverage for, or the MOA can't see the In Basket for the provider they support Issues accessing information with the patient chart <p>Notes:</p> <ul style="list-style-type: none"> User can message in CC to request help when in CCPP. The support for customer service requests is 8-4pm. Anything after there is not current desk that supports outside of hours. Goes to an In Basket and the CCPP monitors and actions In Basket Customer Service Request Types: <ul style="list-style-type: none"> Report a Problem Request for Health Information Access Transfer
6.0 AHS Learning Services (Tier 2)	<p>AHS Learning Services (Tier 2) receives request for CCPP support</p>

receives request for CCPP support from AHS IT Service Desk	<p>from AHS IT Service Desk.</p> <p>The MyLearning Link Support Centre provides end user support for all aspects related to:</p> <ul style="list-style-type: none"> • Course registration • Course completion errors • Navigation of the MLL site <p>MyLearningLink Support MyLearningLink Support Centre is open Monday to Friday 8:30 – 3:30 pm 1-888-580-7010 or helpmylearninglink@ahs.ca.</p> <p>Note: Help documentation is contained within Insite so not accessible to these end-user</p>
7.0 AHS Privacy (Tier 2) receives request for CCPP support from AHS IT Service Desk	<p>AHS Privacy (Tier 2) receives request for CCPP support from the AHS IT Service Desk.</p> <p>The AHS Privacy (Tier 2) provides support for issues such as:</p> <ul style="list-style-type: none"> • CCPP issues/items that involve breach or potential breach under FOIP or HIA • Queries or matters that involve authority for access and disclosure to personally identifying personal and health information
8.0 AHS Provider Bridge (Tier 2) receives request for CCPP support from AHS IT Service Desk	<p>AHS Provider Bridge (Tier 2) receives request for CCPP support from the AHS IT Service Desk.</p> <p>AHS Provider Bridge provides support for issues such as:</p> <ul style="list-style-type: none"> • Receives feedback from users on portal functionality • Email Address: ccproviderbridge@ahs.ca – can be shared with external users • This team answers questions that may arise from the community providers such as: <ul style="list-style-type: none"> ○ What is the difference between Netcare and Connect Care? ○ How does the Connect Care Provider Portal support communities?

4.7 CCPP 180-day Inactive Access Account Disabling

The following actors are part of the CCPP 180-day Inactive Access Account Disabling:

- **AHS IAM (system)**
- **Netcare Access Administrator (NAA)**
- **CCPP User**

4.7.1 Process Flow

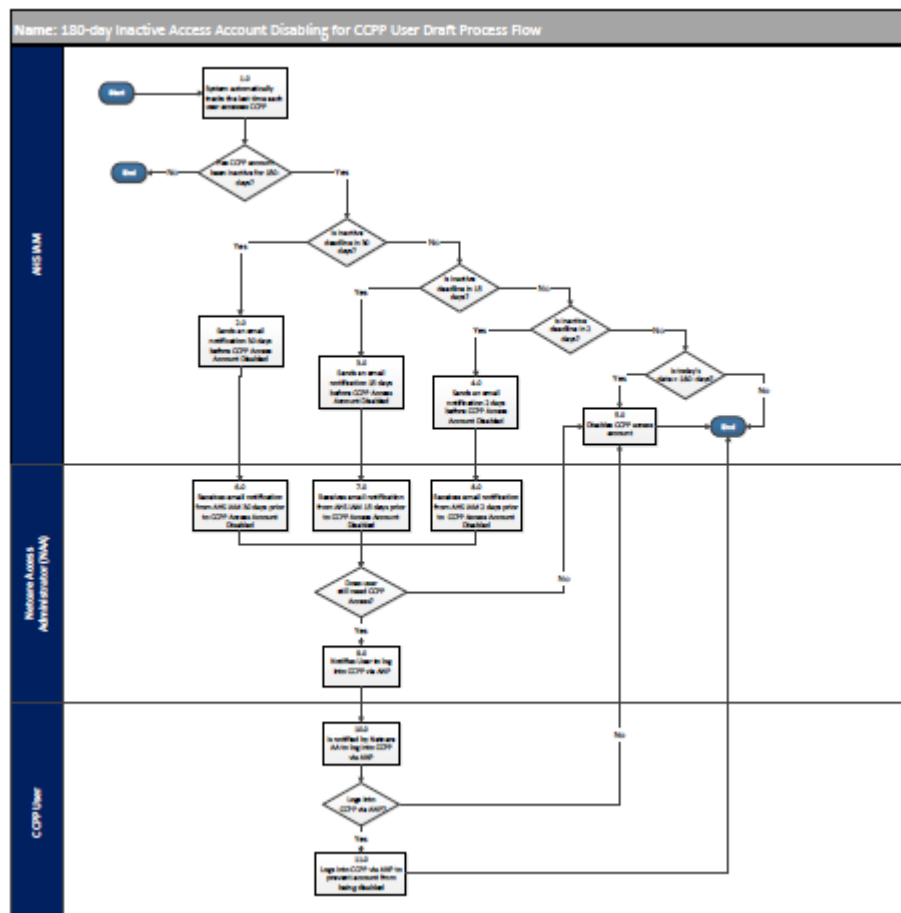


Figure 7- CCPP 180 days Inactive Access Disabling

4.7.2 Process Tasks

Process Flow Number & Name	Task
1.0 System automatically tracks the last time the user has logged into CCPP	System automatically tracks the last time each user accesses CCPP
For each user the system checks to see if the CCPP account has been inactive for 150 days	<p>The system will check access inactivity for CCPP access for each user.</p> <p>Note: A person's ANP access can be active and their CCPP access disabled, but a person's CCPP access cannot be active while their ANP access is disabled. When the ANP access is disabled, their CCPP access becomes disabled as well because ANP access is required to get into CCPP.</p>

	<p>The system checks to see if the CCPP account has been inactive for 150 days.</p> <p>If a user's CCPP account has been inactive for 150 days, then the system checks to see if the active deadline is in 30 days.</p> <p>If the active deadline is in 30 days, then proceed to Step #2 Sends an email notification 30 days before CCPP Access Account Disabled</p> <p>If the active deadline is not in 30 days, then the system checks to see if the active deadline is in 15 days?"</p> <p>If the active deadline is in 15 days, then proceed to Step #3 Sends an email notification 15 days before CCPP Access Account Disabled</p> <p>If the active deadline is not in 15 days, then the system checks to see if the active deadline is in 2 days?"</p> <p>If the active deadline is in 2 days, then proceed to Step #4 Sends an email notification 2 days before CCPP Access Account Disabled</p> <p>If the active deadline is not in 2 days, then the system checks to see if today's date is past the active deadline.</p> <p>If today's date is past the active deadline, then proceed to Step #5 Deactivates CCPP access account.</p> <p>If today's date is not past the active deadline, then the process ends.</p> <p>If a user's CCPP account have not been inactive for 150 days, then the process ends.</p>
2.0 Sends an email notification 30 days before CCPP Access Account Disabled	An automated email notification is sent from the AHS Identity & Access Management (IAM) system, "Identity Management" advising that a CCPP access account(s) is about to be disabled in approximately 30 days.
3.0 Sends an email notification 15 days before CCPP Access Account Disabled	An automated email notification is sent AHS IAM advising that a CCPP access account(s) is about to be disabled in approximately 15 days.
4.0 Sends an email notification 2 days before CCPP Access Account Disabled	An automated email notification is sent from AHS IAM advising that a CCPP access account(s) is about to be disabled in approximately 2 days.
5.0 Deactivates CCPP access account(s)	<p>The system deactivates CCPP access for the CCPP user.</p> <p>Note: Disabled CCPP accounts cannot be 're-activated' — users wishing to regain CCPP access with a disabled account will need to reapply for access, and subject to re-completing the EPIC – ECL200 Introduction to Connect Care Provider Portal training course.</p> <p>The process ends.</p>
6.0 Receives email notification from AHS IAM 30 days prior to CCPP	The Netcare Access Administrator (NAA) receives an automatic email notification from AHS IAM 30 days prior to CCPP Access Account Disabled

Access Account Disabled	
7.0 Receives email notification from AHS IAM 15 days prior to CCPP Access Account Disabled	The Netcare AA receives an automatic email notification from AHS IAM 15 days prior to CCPP Access Account Disabled
8.0 Receives email notification from AHS IAM 2 days prior to CCPP Access Account Disabled	The Netcare AA receives an automatic email notification from AHS IAM 2 days prior to CCPP Access Account Disabled
Does user still need CCPP access?	<p>The Netcare AA determines whether the CCPP user still needs CCPP access</p> <p>If the user still needs CCPP access, then proceed to Step #9.0 Notify User to log into CCPP via ANP</p> <p>If the user does not need CCPP access, then proceed to Step #5 Deactivates CCPP access account</p>
9.0 Notify User to log into CCPP via ANP	The Netcare AA notifies the CCPP user to log into CCPP via ANP to ensure account stay active
10.0 Is notified by Netcare AA to log into CCPP via ANP	The CCPP user is notified by the Netcare AA to log into CCPP via ANP to ensure account stay active
Logs into CCPP via ANP?	CCPP user decides whether to log into CCPP via ANP
11.0 Logs into CCPP via ANP to prevent account from being disabled	<p>The CCPP user logs into CCPP via ANP to prevent account from being disabled.</p> <p>The process ends.</p>

5 Summary of the CCPP via ANP Draft Process Flows

5.1 Existing Netcare Facility – CCPP via ANP For Mixed Context Provider and Staff.

The process begins when a mixed context provider (Lead Custodian), from a community site, decides to request access to the Connect Care Provider Portal (CCPP) via ANP for themselves (if CCPP access is not already granted), and their community clinic staff to support patient care. The process begins when the mixed context provider (Lead Custodian) expresses interest, either through eHealth Services (eHS) or by the Netcare Access Administrator (NAA) directly submitting an ANP request for CCPP via AHS IAM.

If the mixed context provider goes through eHS typically it is by phone or email, and eHS becomes aware of the new inquiry either through the Contact Centre (CC) or could be received directly to eHS Service area. With the bundled services approach, there is a new Coordinating Agent (CA) role which is the streamlined point of contact between the mixed context provider (Lead Custodian) and eHS. When eHS receives a request for CCPP via ANP, the required information is obtained, then passed onto the CA. As part of the Intake process, eHS Privacy and Security ensures the PIA Letter is complete and the pORA is up to date. If either of these need to be updated, eHS Privacy and Security support is provided to meet PIA and pORA requirements. eHS Privacy and Security also works with the Provider/Lead Custodian to complete the CCPP Access Agreement for each Custodian that is requesting CCPP access via ANP. With the new transformation and CA role all forms are pre-completed by the CA including the CRF. The CA checks to see if the facility is live within AHS IAM and provides support with the CRF process if it is not. As part of completing the CRF process, the eHS Forms Management Services adds the W DFA to the ANP Rollout List in AHS IAM and sends out the AHS IAM Username to the Netcare Access Administrator (NAA) Role(s). eHS then provides NAA registration and training support for new NAA's or AA refreshing training for existing NAA's.

The next step, whether going through eHS or directly to AHS IAM, the NAA submits an ANP request for CCPP via AHS IAM. This starts the processes of Netcare and CCPP access and sends a notification to the eHS forms work queue (TBD). This notification alerts eHS which allows eHS to ensure the privacy and security requirements are met even when the NAA submits the ANP request directly in AHS IAM.

From here AHS IAM creates the AD account and sends the CCPP role to AHS LDAP. AHS LDAP sends the role to MyLearning Link and then the mixed context provider and/or staff completes the CCPP training. Once the CCPP training is completed, AHS LDAP is notified from MyLearningLink the training has been completed by the CCPP user. Then AHS IAM provisions ANP/CCPP and AD group and sends automated notification to the NAA. The AHS Connect Care Provider Portal IT Team then receives an automated notification that the CCPP user has completed the required training and manually adds User Context to EMP Managed Access setting.

The NAA receives AHS IAM automated notification that CCPP is provisioned, then notifies the mixed context provider and staff. Next the mixed context provider and staff submit personal

information, such as address and gender and into an AHS IAM questionnaire. This information is required for the Connect Care Smart Audit Tool to operate. The last step involves the mixed context provider and staff then log into ANP and accesses CCPP successfully.

5.2 Net New Netcare Facility – CCPP via ANP for Mixed Context Provider

As part of requesting Netcare access, this process begins when a mixed context provider (Lead Custodian), from a community site, decides to also request access to the Connect Care Provider Portal (CCPP) via ANP for their community clinic staff to support patient care. The process begins when the mixed context provider (Lead Custodian) expresses interest, typically through phone or email, and eHS becomes aware of the new inquiry to the Contact Centre (CC). With the bundled services approach, there is a new Coordinating Agent role which is the streamlined point of contact between the mixed context provider (Lead Custodian) and eHealth services. When the Contact Centre receives a request for CCPP via ANP, the Contact Centre obtains the required information, then passes this information onto the Coordinating Agent. As part of the Intake process, eHS creates the facility within Customer Relationship Management (CRM) and initiates the Onboarding Request (OR) process. Additionally, the eHS privacy and security services assist in addressing privacy and security requirements, such as Privacy Impact Assessment (PIA), Provincial Organizational Readiness Assessment (pORA) and User Agreement/Netcare IMA. eHS provides Netcare Access Administrator (NAA) registration and training support for new Netcare AA's and the mixed context provider/Lead Custodian completes facility and CCPP user privacy/security requirements and access registration.

Next the NAA submits an ANP request for CCPP via AHS IAM and this starts the processes of Netcare and CCPP access. From here AHS IAM creates the AD account and sends the CCPP role to AHS LDAP. Next the mixed context provider and staff submit personal information, such as address and gender, into an AHS IAM questionnaire. The AHS LDAP sends the role to MyLearning Link and then the mixed context provider and/or staff completes the CCPP training. Once the CCPP training is completed, AHS LDAP is notified from MyLearningLink the training has been completed by the CCPP user. Then AHS IAM provisions ANP/CCPP and AD group and sends automated notification to the NAA. The AHS Connect Care Provider Portal IT Team then receives automated notification that the CCPP user has completed the required training and manually adds User Context to EMP Managed Access setting.

The NAA receives AHS IAM automated notification that CCPP is provisioned, then notifies the mixed context provider and staff who then log into ANP and accesses CCPP successfully.

5.3 CCPP User Offboarding

The process begins when the mixed context provider or Lead Custodian of the existing Netcare facility notifies to offboard CCPP user. This can be initiated either by contacting eHS Contact Centre by phone or email or by the Netcare Access Administrator (NAA) submitting a request through AHS IAM.

If the CCPP Offboarding request come through eHS the following extra steps are performed:

- With the bundled services approach, there is a new Coordinating Agent role which is the streamlined point of contact between the mixed context provider or Lead Custodian and

eHealth services therefore when the Contact Centre receives a request to remove CCPP via ANP access, the Contact Centre obtains the required information, then passes this information onto the Coordinating Agent.

- The eHS Services provides CCPP support.

The NAA submits an ANP request to deselect CCPP access in AHS IAM and the ANP request is processed. There is a direct API with Epic which will remove the template for CCPP and inactivates the account (if it is the last template). The connector with Active Directory will also remove the CCPP AD group. If the end-user only has AD for CCPP access the AD account will also be disabled at this time. A work item will then be generated for the Connect Care Provider Portal IT Team and this team removes the CCPP user context from the end user EMP and if the CCPP user is a prescriber then the CCPP user would also be removed from the Provider Group as well. The AHS IAM system sends an automated notification to the NAA informing of the removal of the CCPP Access for the specified custodian. The last step performed will be the NAA receives an automated notification from the AHS IAM system that CCPP access has been removed for the specified custodian.

5.4 OCME Netcare/CCPP Onboarding

The following two pre-conditions have to be done prior to users requesting CCPP access:

- CCPP Access Agreement has been completed and signed by the Netcare AA (HIAPPSU)
- PIA Endorsement Letter has been signed by the Netcare AA (HIAPPSU)

The process begins when OCME initiates onboarding by emailing a list of eligible staff details to the eHS Support Privacy and Security Lead via eHS OCME dedicated mailbox. The eHS Privacy and Security lead enters this information into the encrypted OCME User Tracker stored in Ensemble/AH Sharepoint. Each OCME User must submit a signed Affiliate Acknowledgement document to the eHS OCME dedicated mailbox. The eHS Privacy and Security lead uploads the signed Affiliate Acknowledgment document into SharePoint.

The OCME User must enroll in HIA General Awareness Training held on the third Wednesday of each month by sending an email to the HIA Help Desk and cc to eHS OCME dedicated mailbox.

HIAPPSU (Director and Team) tracks OCME User's enrollment in the HIA General Awareness Training and enters information in the HIA Training spreadsheet by Alberta Health. The OCME User completes the HIA General Awareness Training and sends an email to the HIA Help Desk to notify the training has been completed. HIAPPSU (Director and Team) tracks OCME Users completion of HIA General Awareness Training and enters information in the HIA Training spreadsheet by Alberta Health.

The eHS Privacy and Security lead will send an email to the HIA training organizers to confirm the list of the OCME users that completed the training and then will add the users to the encrypted OCME User Tracker stored in Ensemble by eHS Privacy and Security lead. The eHS Privacy and Security lead will advise the Director, HIAPPSU via email that the Affiliate Acknowledgement are awaiting signature in SharePoint.

The Director, HIAPPSU will sign the Affiliate Acknowledgement on behalf of the Department and will store a final copy in SharePoint. The eHS Privacy and Security lead will update the

Encrypted OCME User's Tracker stored in Ensemble.

At the OCME's request, the eHS Privacy and Security lead will provide OCME copies of the Affiliate Acknowledgement signed by both the OCME User and Alberta Health stored in SharePoint. Once HIA General Awareness Training is complete, and the Affiliate Acknowledgement has been signed, the eHS Privacy and Security lead will provide the eligible OCME User information to the eHS training team to begin the process of providing Netcare Training to the OCME Users. The eHS Privacy and Security lead will inform the eHS Training Services lead that new OCME users are ready for training with preference to have a training session dedicated to a group of OCME users only and offer the option to join a regular training session for the rest of the OCME users unable to join the dedicated session. Then the OCME User completes the Netcare Training. When an OCME User's Netcare training has been completed, they will email the User Registration Form (URF) and Smart Auditing Tool (SAT) information to the dedicated eHS OCME mailbox.

eHS Privacy and Security lead will confirm that the URF and SAT information are complete after internal QA process, will ensure that HIA training and affiliate acknowledgement is complete on the Encrypted OCME User's Tracker stored in Ensemble. and will forward it to Alberta Health's Access Administrator (AA) who will review and process through AHS IAM. The HIAPPSU Access Administrator (AA) reviews and processes the Netcare/CCPP access credentials through AHS IAM.

The Netcare AA enters the SAT information for each CCPP user at that facility within a spreadsheet and then sends the spreadsheet within an encrypted email to AHS Medical Affairs. AHS Medical Affairs enters the CCPP user's information into Application & Privileging (A&P) which is sent to AHS LDAP.

This starts the processes of Netcare and CCPP access. From here AHS IAM creates the AD account and sends the CCPP role to AHS LDAP. Then AHS LDAP sends the role to MyLearning Link. Next the OCME User completes the CCPP training (On Our Best Behavior (OOBB) and the ECL 200 Introduction to CCPP). Once the CCPP training is completed, AHS LDAP is notified from MyLearningLink the training has been completed by the CCPP user. Then AHS IAM provisions ANP/CCPP and AD group and sends automated notification to the Netcare AA. The AHS Connect Care Provider Portal IT Team then receives manual notification that the CCPP user has completed the required training and manually adds User Context to EMP Managed Access setting.

The Netcare AA receives AHS IAM automated notification that CCPP is provisioned, then notifies the OCME user a credential notice email to provide OCME User's Netcare/CCPP access, with cc to eHS Privacy and Security lead. The OCME user then log into ANP and accesses CCPP successfully. The last step in the process is eHS Privacy and Security confirms with OCME that credentials were received and log-in was successful.

5.5 OCME Netcare/CCPP User Offboarding

The process begins when the OCME notifies eHS Privacy and Security lead to remove Netcare/CCPP access for an OCME user. eHS Privacy and Security lead notifies Alberta Health (AA) to remove OCME user's Netcare/CCPP access via email. The Alberta Health AA then submits an ANP request to remove Netcare/CCPP access in AHS IAM and the ANP request is

processed. There is a direct API with Epic which will remove the template for CCPP and inactivates the account (if it is the last template). The connector with Active Directory will also remove the CCPP AD group. If the end-user only has AD for CCPP access, the AD account will also be disabled at this time. A work item will then be generated for the Connect Care Provider Portal IT Team and this team removes the CCPP user context from the end user EMP and if the CCPP user is a prescriber then the CCPP user would also be removed from the Provider Group as well. The AHS IAM system then sends an automated notification to the Alberta Health (AA) informing of the removal of the Netcare/CCPP access for the specified custodian. Next the Alberta Health (AA) receives an automated notification from the AHS IAM system that Netcare/CCPP access has been removed for the specified custodian. The last step in the CCPP offboarding process is the eHS Privacy and Security lead will update the Encrypted OCME User's Tracker stored in Ensemble to indicate that the user access was deleted.

5.6 CCPP Support Draft Workflow

When a Netcare/CCPP user requires CCPP Support, contact is made to one of the following services:

- eHealth Services Contact Centre
 - By Phone (1-855-643-8649)
 - By Email (eHealthProviderSupport@gov.ab.ca)
- AHS IT Service Desk (Tier 1)
 - By Phone (1-877-311-4300)
- Provincial Service Desk (Tier 1)
 - By Phone (1-877-931-1638)

Where the Netcare/CCPP user is working will determine which support team to call.

- If the Netcare/CCPP user is working at a community facility, the eHealth Services Contact Centre will be contacted.
- If the Netcare/CCPP user is working at an AHS facility, then the AHS IT Service Desk will be contacted.
- If the Netcare/CCPP user needs a Netcare password reset, then the Provincial Service Desk will be contacted.

Note:

All three of these teams work closely together and their top priority is to resolve issues that the Netcare/CCPP user has. If the Netcare/CCPP user contacts the wrong service desk, the Netcare/CCPP user will be redirected to the appropriate team according to the type of issue.

Each team is responsible for certain tasks.

1. eHealth Services Contact Centre

eHS is responsible for handling the following:

- Privacy and Security Services Support
- CCPP Training and Registration Services Support

2. AHS IT Service Desk

The AHS IT Service Desk (Tier 1) is responsible for handling the following:

- AHS IAM technical difficulties
- Netcare password reset (Combo role type only)
- RSA access issues
- Main line that can triage to the CCPP team, but not to the AHS Bridge team
- CCPP user has access to CCPP, but cannot log in
- Technical issue with MyLearningLink (MLL) – includes MLL password resets
- MLL Login issues after receiving their MLL (AD) login credentials (possibly due to MFA issues). On the MLL login page external users should be able to utilize the **Update/Change your Password** (if the current password is known) feature, but the **Forgot Your Password?** option is only available if the user is connected to AHS either through RSA, VPN or if at an AHS site. The reason for this is the resource is connected to the IAM system.
- Azure multi-factor authentication

3. Provincial Service Desk

The Provincial Service Desk (Tier 1) is responsible for handling the following:

- Netcare password reset (Community role type only)
- Triage CCPP registration and training questions

For issues that go to the AHS IT Service Team, if they cannot be resolved at the Tier 1 level, the CCPP user will then be redirected to one of the following Tier 2 team within their organization:

- AHS Connect Care Provider Portal IT Team
- AHS Learning Services
- AHS Privacy
- AHS Provider Bridge

AHS Connect Care Provider Portal IT Team is responsible for the following:

- Issues with access to CCPP (i.e. access denied, other login issues, site could not be reached, etc.)
- Help with functionality questions e.g. can't see In Basket for MOA they are providing coverage for, or the MOA can't see the In Basket for the provider they support
- Issues accessing information within the patient care

AHS Learning Services is responsible for the following:

- Course registration
- Course completion errors
- Navigation of the MLL site

AHS Privacy is responsible for the following:

- CCPP issues/items that involve breach or potential breach under FOIP or HIA
- Queries or matters that involve authority for access and disclosure to personally identifying personal and health information

AHS Provider Bridge is responsible for the following:

- Receive feedback from users on portal functionality
- Email Address: ccproviderbridge@ahs.ca – this email can be shared external
- This team answers questions that may arise from the community providers such as:
 - What is the difference between Netcare and Connect Care
 - How does the Connect Care Provider Portal support communities?

5.7 CCPP 180-day Inactive Access Account Disabling

When a person has not logged into Alberta Netcare Portal for 180 consecutive days (approximately 6 months), their ANP access account will be disabled. They will not be able to log into ANP. Similarly, when a person has not logged into Connect Care Provider Portal for 180 consecutive days (approximately 6 months), their CCPP access account will be disabled, and they will not be able to log into CCPP.

Note: A person's ANP access can be active and their CCPP access disabled, but a person's CCPP access cannot be active while their ANP access is disabled. When the ANP access is disabled, their CCPP access becomes disabled as well because ANP access is required to get into CCPP.

Automated email notifications will be sent from the AHS IAM system advising that an CCPP access account is about to be disabled in approximately 30, 15 and 2 days. These email notifications will be sent to the person who authorized CCPP access for the end-user. AHS end-users of CCPP will be sent notifications provided AHS IAM has a valid email address for the CCPP user. Community end-users of CCPP will not be sent email notifications, only their Netcare AA will be notified.

Netcare AA can decide whether the user still needs CCPP access. If the CCPP user still needs access, then the Netcare AA should get in touch with the CCPP user and request that they log in to CCPP via ANP to prevent the CCPP access account from being disabled. If the CCPP user no longer needs CCPP access, then the CCPP account will be disabled when the CCPP user does not log in after 180 days.

Once the CCPP user is notified by the Netcare AA, the CCPP user logs into CCPP via ANP to prevent the CCPP account from being disabled. If the CCPP user does not log into CCPP via ANP within the 180 days, then the CCPP account will be disabled.

Note:

Disabled CCPP accounts cannot be 're-activated' — users wishing to regain CCPP access with a disabled account will need to reapply for access, and subject to re-completing the EPIC – ECL200 Introduction to Connect Care Provider Portal training course.

6 Terms, Acronyms, and Abbreviations

Provide a list of the key terms, acronyms, and abbreviations used in this document.

Term/Acronym	Description
AD	Active Directory
AH	Alberta Health
AHS	Alberta Health Services
AHS IAM	Alberta Health Services Identity Access Management
ANP	Alberta Netcare Portal
A&P	Application & Privileging
CA	Coordinating Agent
CCPP	Connect Care Provider Portal
CRF	Custodian Registration Form
CRM	Customer Relationship Management
DSR	Delivery Site Registry
eHS	eHealth Services (CGI)
HIA	Health Information Act
HIAPPSU	HIA Policy, Privacy and Security
IEP	Information Exchange Protocol
IMA	Informational Manager Agreement
LPR	Limited Production Rollout
MLL	My Learning Link
NAA	Netcare Access Administrator
NAR	Network Activation Request
OCME	Office of the Chief Medical Examiner
OIPC	Office of the Information and Privacy Commissioner
OR	Onboarding Request
OU	Organizational Unit

Term/Acronym	Description
PIA	Privacy Impact Assessment
pORA	Provincial Organizational Readiness Assessment
P&S	Privacy & Security
RUNA	Remote User Network Access
SAT	Smart Auditing Tool
UAP	Unified Access Portal
URF	User Registration Form
WDFA	The 4-digit number that each site receives and is generated by the Delivery Site Registry (DSR)

7 References

Provide a list of the other documents referenced in this document.

File Name and Location	Description
<AHS Process Steps>	

8 Appendix A – MLL Welcome Email Template

This email is to inform you that you have been granted access to MyLearningLink (MLL), Alberta Health Services' provincial learning management system. MLL hosts the online eLearning courses users must complete before they are authorized to access the Connect Care Provider Portal (CCPP) via ANP.

Before being granted access to the Connect Care Provider Portal, you must complete two learning modules.

1. InfoCare - On Our Best Behaviours. This course is AHS' mandatory privacy and information security training and acceptance of the AHS Confidentiality & User Agreement.
2. Epic - ECL200 Introduction to Connect Care Provider Portal. This course provides instructions on how to use the CCPP.

Accessing MyLearningLink

1. Go to <https://myapps.albertahealthservices.ca>
2. Log into MyApps using your AHS user ID and AHS password.
3. Find the MyLearningLink – EMR Users tile on the Apps page.
4. The RSA SecurID token authentication window appears. Enter your RSA passcode from your soft token app on your device.
5. You will be presented with the MyLearningLink login page. Enter your AHS user ID and AHS password, and click LOG IN.*

If you have issues with MyApps, RSA SecurID token authentication or need ID and password assistance, contact AHS' IT Service Desk & Solution Centre at 1-877-311-4300:

- Select option 1 for Clinical Applications, and then select option 1 for Connect Care

Accessing Your Training in MyLearningLink

1. On the left-hand side under the MLL logo, click on Learning Home.
2. Next click on Required Courses. This will bring up a page with your assigned role. The courses listed under Required Courses (except for Alberta Health Services Employees: Required Organizational Learning. These courses are for AHS staff only) are based on your assigned role. Note, this page may load slowly.
3. Click on the Role (blue bar) and then click on Track 1 (gray bar) to display the courses required to complete the training for that role.
4. Register for the course by clicking the green Register button. Complete the course.

For questions about your Connect Care Provider Portal role and required training or if your role is incorrect, discuss with your clinic's Netcare Access Administrator (NAA).

Browser and Hardware Compatibility

MyLearningLink is available on all browsers including mobile devices. However, courses are designed for AHS IT Browser Standard Microsoft Edge. To optimize your experience, we suggest that you complete your training using Microsoft Edge in Windows 10 on a desktop or laptop computer.

If your personal computer or device does not adhere to these standards, experience may vary.

MyLearningLink Support

For questions about MyLearningLink, contact the MyLearningLink Support Centre at helpmylearninglink@albertahealthservices.ca.

*The collection of your personal information by the MyLearningLink site is legally authorized by section 33(c) of the Freedom of Information and Protection of Privacy Act (Alberta). Your information will only be used and disclosed as necessary to support and manage your learning experience, including registration and the reporting of course completion. If you have any questions about the collection of your personal information by MyLearningLink, please contact Learning Services by emailing HelpMyLearningLink@albertahealthServices.ca, or calling 1-888-580-7010.

Privacy and Security Support Process CCPP via ANP

Ministry

Alberta Health

Division Name:

Health Information Systems

Branch/Unit:

Strategic IMT Services

Creation Date:

November 25, 2024

Print Date:

February 19, 2025

Document Version:

1.0

Template Location

Primary Contact:	Project Management Office (PMO)	Health.PMO@gov.ab.ca
Template Location:	The master copy of this template is located in the PMO Framework HealthShare Site.	
Template Version	V 1.0.2	
Template Date	May 28, 2014	

Template Usage

This template is being provided by Alberta Health through the PMO, Information Management Branch of Health Information Systems (HIS) Division to provide a common and consistent approach for the delivery of IT-related initiatives and projects.

Some sections of the template may contain *italicized* descriptive information that should be removed once the template has been filled in.

Some projects may require additional elements be added to the deliverable, additional elements may be inserted throughout the document as appropriate. **Note: Removing template sections may introduce risk and potentially affect the success of the project. In the event that a section is not applicable to your project, a brief explanation should be provided as to why it is not applicable.**

Deliverables should wherever possible, be provided in MS Word format. Embedded objects such as diagrams and charts should be created using a common or standard tool such as MS Word and MS Visio and the source objects should be available rather than just a snapshot of the objects.

Your opinion and suggestions for improving this template are important to the PMO, Health Information Systems Division (HIS). The PMO has instituted a review and release process to help improve the templates. Contact the PMO to learn how your input to continuous improvement can be captured.

Table of Contents

DOCUMENT LOCATION	4
DOCUMENT REVISION HISTORY	4
DELIVERABLE APPROVERS AND REVIEWERS	4
1 DOCUMENT PURPOSE	6
1.1 BACKGROUND	6
1.2 CURRENT STATE	6
1.3 TARGET STATE.....	6
2 PRIVACY AND SECURITY STEPS FOR CCPP ONBOARDING VIA ANP FOR MIXED-CONTEXT PROVIDERS (PHYSICIANS, NURSE PRACTITIONERS) AND THEIR STAFF	8
2.1 ROLES COVERED	8
2.2 PROCESS OVERVIEW.....	8
3 SUMMARY FOR CCPP VIA ANP ONBOARDING PROCESS.....	ERROR! BOOKMARK NOT DEFINED.
4 OCME VIA ANP USER REQUIREMENTS AND PROCESS	13
5 TERMS, ACRONYMS, AND ABBREVIATIONS	19
6 REFERENCES	21

Document Location

Document Revision History

Version	Version Date	Summary of Changes	Author
0.1	November 25, 2024	Initial Draft	Soumeya Movaffagh
0.2	December 10, 2024	Revised based on feedback from AH and AHS	Soumeya Movaffagh
1.0	February 13, 2025	Finalized document	Lloyd Thorpe

Note: Removing template sections may introduce risk and potentially affect the success of the project. In the event that a section is not applicable to your project, a brief explanation should be provided as to why it is not applicable.

Deliverable Approvers and Reviewers

Use the following table to name the deliverable approvers and reviewers. Deliverable approvers and reviewers should be the same as those already stated in the Project Management Plan for this deliverable.

Title and Name	Type	Purpose
Lloyd Thorpe Senior Project Manager, eHealth Ecosystem Modernization, AH	A	<i>Reviews and approves</i>
Verica Jelic EHR Deployment Manager, AH	A	<i>Reviews and approves</i>
Sheri Ross Senior Clinical Specialist, AH	A	<i>Reviews and approves</i>

Title and Name	Type	Purpose
Amanda Harrigan Policy Advisor HIA, AH	<i>A</i>	<i>Reviews and approves</i>
Brian Hamilton Privacy & Security Lead / SME eHealth Services, CGI	<i>R</i>	<i>Reviews</i>
Tara England Director, Consulting Services, eHS Operations Manager, CGI	<i>R</i>	<i>Reviews</i>
Rorisang Hlahatsi-Baloyi Senior Management Consultant, Emerging Technology, CGI	<i>I</i>	<i>Informed</i>

Type: *A* – Approves (implies review as well); *P* – Prepares; *R* – content review and input; *I* – Information Only

1 Document Purpose

The purpose of this document is to define the Privacy and Security Support (PSS) process for mixed-context providers, their staff, and Office of the Chief Medical Examiner (OCME) users to obtain secure, compliant access to Connect Care Provider Portal (CCPP) via the Alberta Netcare Portal (ANP). This process ensures alignment with legislative and organizational requirements, enabling authorized users to access, manage, and utilize electronic health information effectively.

1.1 Background

The Connect Care Provider Portal (CCPP) is a web-based application that allows clinicians and staff (from community sites and OCME) with appropriate role-based access to securely access the health information from Connect Care.

It is designed to improve the continuity of care for patients as they move between sites in AHS and their primary care providers in the community. Clinicians who currently use Alberta Netcare Portal (ANP) will be able to access CCPP via an in-context launch from a tab in ANP.

Previously, AH and AHS collaborated on a project to enable ANP enabled care providers logged in to ANP to launch in context to CCPP (single sign on).

The project was stalled as a result of OIPC feedback regarding the authority identified by AHS for managing the sharing of CCPP patient information to clinicians who are not AHS affiliates.

ADM/Sr. ADMAH direction is to move forward with implementation preparations and deploy to a limited number of users in the Limited Production Rollout (LPR) within the January 2025 timeframe.

1.2 Current State

At present, mixed context providers—those working within AHS and community clinics—may have Connect Care access but their clinic staff do not, which can create challenges when coordinating patient follow-ups. Additionally, while users in the Office of the Chief Medical Examiner (OCME) have Netcare access, they currently lack access to CCPP, limiting their ability to review comprehensive patient records.

1.3 Target State

The CCPP via ANP project aims to expand access to CCPP for community providers and their clinic staff, with an initial focus on mixed context providers. This will improve patient care by ensuring continuity of health information across both AHS and community settings. Alberta Health will make CCPP information available via ANP under the authority of section 56.3(6) of the Health Information Act (HIA). As such, CCPP will be added to the scope of the Alberta Electronic Health Record initiative. Alberta Health acts as the information manager for the Alberta Electronic Health Record under section 2 of the Alberta Electronic Health Record Regulation. As the information

manager for the Alberta Electronic Health Record, Alberta Health has assigned its eHealth Services team to manage user deployment processes for both ANP and CCPP.

This project will include:

- Deployment to Community Providers: Extending CCPP access to community providers and their staff, starting with mixed context providers.
- Deployment to OCME Users: Extending CCPP access to OCME staff, with tailored onboarding and support processes to ensure seamless integration.

By achieving these objectives, the CCPP via ANP project will significantly enhance healthcare delivery, promote the availability of comprehensive health data, and streamline the integration of health information across Alberta's health system.

2 Privacy and Security Steps for CCPP Onboarding via ANP for Mixed-Context Providers

This document outlines the privacy and security steps required for community clinics and their staff (physician offices and nurse practitioner practice sites) to access the Connect Care Provider Portal (CCPP) via the Alberta Netcare Portal (ANP). This ensures compliance with privacy and security regulations while verifying the clinic's readiness to access sensitive health information.

2.1 Roles Covered

The CCPP Onboarding Process applies to the following roles:

- Lead Authorized Custodian (must meet “authorized custodian” criteria in s. 3 of Alberta Electronic Health Record Regulation)
- Other Authorized Custodians
- Access Administrator
- Authorized Staff (affiliates of Authorized Custodians)

2.2 Process Overview

The integration of the Connect Care Provider Portal (CCPP) with the Alberta Netcare Portal (ANP) enables community providers, their clinical staff, and the Office of the Chief Medical Examiner (OCME) affiliates to securely access patient health information within the Alberta Electronic Health Record (EHR). This initiative is designed to enhance the continuity of care by providing a more comprehensive view of patient health records.

The scope of this project includes the phased deployment of CCPP access, initially available to mixed-context providers, their clinical staff (including regulated and non-regulated professionals), and OCME affiliates. Access is controlled through strict privacy and security measures, including role-based access control via the Alberta Netcare Permission Matrix, which ensures that only eligible individuals can access the CCPP.

This process is governed by several privacy and security frameworks, including the Health Information Act (HIA) and the Alberta Electronic Health Record Regulation, which ensure compliance with Alberta's privacy laws. The Alberta Health Services (AHS) Identity Access Management (IAM) system is used to administer and manage user access, ensuring that only authorized individuals can access CCPP through the ANP platform.

To maintain security, the CCPP system undergoes regular monitoring and auditing to detect unauthorized access or breaches. Detailed logs are maintained to capture all user interactions with patient data, ensuring accountability and enabling investigation in case of security incidents. Additionally, users must complete a series of mandatory steps, including signing the CCPP Access Agreement, before being granted access.

As part of ongoing risk mitigation, AHS conducts regular vulnerability assessments and ensures that all privacy and security protocols are adhered to in accordance with the Alberta Health Information Management and Security directives. This integrated approach helps protect

sensitive health information while supporting healthcare professionals in providing the best possible care to patients.

Step-by-Step Process:

➤ Existing Netcare Facility – CCPP via ANP for Mixed Context Providers and Staff

Step 1.0: Mixed Context Provider/Lead Custodian Expresses Interest

- Mixed context provider/Lead Custodian expresses interest in accessing CCPP via ANP from the community site.
- Request can be made via eHealth Services (phone/email) or directly through AHS IAM.
- If initiated through eHS, proceed to Step 2.0. If initiated through AHS IAM, proceed to Step 7.0.

Step 2.0: Initial Contact via eHS

- The eHS Coordinating Agent (CA) becomes the main point of contact.
- The eHS Contact Centre/Service area gathers required information and forwards it to the CA to follow-up and complete the Intake.

Step 3.0: Privacy and Security Services (PSS)

- PSS guides the lead and authorized custodian and ensures completion of the PIA endorsement letter, Privacy and Security Risk Assessment, CCPP Access Agreement, Netcare IMA (if not on file), and checks if pORA is reflecting the clinic's current state.

- **PIA:**

The lead custodian will:

- Review Addendum 9 Document.
- Confirm privacy policies and procedures are up to date.
- Complete combined ANP and CCPP endorsement letter and submit to the Information and Privacy Commissioner (OIPC).
- Confirm receipt of PIA Acknowledgement and submit to eHS.

Privacy and Security Self-Assessment:

The lead custodian will:

- Review and sign the Self-Assessment form on behalf of the clinic's custodians.
- Submit the signed Self-Assessment form to eHS via email to eHealthPrivacy@gov.ab.ca for review and storage.

Step 4.0: Sign CCPP Access Agreement and Epic Addendum

- All the authorized Custodians must sign and submit the CCPP Access Agreement and Epic Addendum.
- Obtain the **CCPP Access Agreement** and **Epic Addendum** forms from the **eHealth Consultant**.
- Have all **authorized custodians** sign the documents.
- Submit the signed forms to eHealthServices@gov.ab.ca for tracking and processing and storing in AH's share Point.

Step 5.0: Sign Informational Manager Agreement (IMA) and Review Information Exchange Protocol (IEP)

- For any authorized custodian without an IMA on file:
 - eHS will provide the IMA and IEP forms with instructions for review, signing and submission to the Alberta Health HIA Policy, Privacy, and Security Uni (HIAPPSU).

Step 6.0: Check the Provincial Organization Readiness Assessment (pORA)

- If required, eHS will check and update the pORA ensuring it is reflecting current state.
- eHS will Submit the pORA on behalf of the lead custodian to Alberta Health HIA Policy, Privacy, and Security Uni (HIAPPSU) for review and approval.

➤ Net New Netcare Facility – CCPP via ANP for Mixed Context Providers and Staff**Step 1.0: Mixed Context Provider/Lead Custodian Expresses Interest**

- Mixed context provider/Lead Custodian expresses interest in Netcare and CCPP access (for self and/or clinic staff).
- Request made via phone or email to eHS Contact Centre.

Step 2.0: Initial Contact via eHS

- Coordinating Agent (CA) is assigned as the main point of contact.
- Contact Centre gathers initial details and forwards them to the CA for follow-up.

Step 3.0: Facility DSR/Management Services Create Site in CRM

- DSR Notification is received, and a site is created in CRM for onboarding.
- CA reviews eligibility of the requestor as an authorized custodian via professional college websites.
- Confirm contact details and registration requirements with the clinic.

Step 4.0: Privacy and Security Services

PIA:

The lead custodian will:

- Review Addendum 9 Document.
- Ensure privacy policies are up-to date and reflect your current systems, practices and privacy and security management.

Tip: Contact your health professional college/association to get a model policy set you can customize.

- Individualize the combined ANP and CCPP endorsement letter.
- Submit the combined ANP and CCPP endorsement letter and HIA Policies to the Information and Privacy Commissioner (OIPC).

Tip: Send your PIA via courier and request a signed receipt or email your PIA to the Commissioner at pia@oipc.ab.ca. Both options provide proof that your PIA has been submitted.

- Email the eHealth Services team at: eHealthPrivacy@gov.ab.ca Confirming that combined ANP and CCPP endorsement letter has been submitted to the OIPC, attaching a scan of your signed cover letter.

- **Privacy and Security Self-Assessment:**

The lead custodian will:

- Review and sign the Self-Assessment form on behalf of the clinic's custodians.
- Submit the signed Self-Assessment form to eHS via email to eHealthPrivacy@gov.ab.ca for review and storage.

- **Sign CCPP Access Agreement and Epic Addendum:**

- Authorized Custodians must sign and submit the CCPP Access Agreement and Epic Addendum.
- Obtain the **CCPP Access Agreement** and **Epic Addendum** forms from the **eHealth Consultant**.

- Have all **authorized custodians** sign the documents.
- Submit the signed forms to eHealthServices@gov.ab.ca for tracking and processing.

Step 5.0: Sign Informational Manager Agreement (IMA) and Review Information Exchange Protocol (IEP)

- For authorized custodians without an IMA:
 - eHS will provide the IMA and IEP forms with instructions for review, signing and submission.

Step 6.0: Complete Provincial Organization Readiness Assessment (pORA)

- complete a new pORA for the community facility to meet security standards.
- Submit completed pORA for review and approval by Alberta Health.
- **Outcome: pORA approval** and a signed confirmation from Alberta Health. The **pORA** is valid for two years and must be updated thereafter.

3 OCME CCPP VIA ANP User Requirements and Process

Background

In November 2023, Alberta Health and Alberta Justice and Solicitor General finalized a new Memorandum of Understanding (MOU) regarding Netcare Access for Office of the Chief Medical Examiner (OCME) Users. The MOU acknowledges that OCME Users will be given access to Alberta Netcare as affiliates of Alberta Health. Under the MOU, OCME Users are authorized to access Alberta Netcare and copy information from it to carry out their duties under the Fatality Inquiries Act (FIA).

In conjunction with the new MOU, Alberta Health has asked **eHealth Support (eHS)** to take over administration of the OCME User registration process, which was formerly handled by the Health Information Act Policy, Privacy, and Security Unit.

Purpose

To delineate the **eHS process** for granting **ANP access** to OCME Users in alignment with the new MOU, including **CCPP access** for OCME users.

OCME Netcare/CCPP Onboarding Process

1.0 Email eligible staff to eHealth Support Privacy and Security Lead

- OCME provides a list of eligible staff to eHealth Support Privacy and Security Lead via the OCME dedicated mailbox CA.SM.PRJ.eHealth.OCME@cqi.com
- The email includes the staff member's name, job role, regulated health profession, and office location.

2.0 Enter information into the Encrypted OCME User's Tracker

- eHS Privacy and Security Lead enters the provided staff details into the Encrypted OCME User Tracker stored in Ensemble/AH SharePoint.

3.0 Submit signed Affiliate Acknowledgement

- Each OCME User sends a signed Affiliate Acknowledgement document to the eHS OCME dedicated mailbox.

4.0 Upload signed document into SharePoint.

- eHS Privacy and Security Lead uploads the signed Affiliate Acknowledgement document into SharePoint.

5.0 Enroll in HIA General Awareness Training

- The OCME User enrolls in HIA General Awareness Training by emailing the HIA Help Desk and cc'ing the eHS OCME mailbox.

6.0 Track HIA Training enrollment

- HIAPPSU tracks OCME User's HIA General Awareness Training enrollment and updates the HIA Training spreadsheet.

7.0 Complete HIA General Awareness Training

- OCME User completes the training and sends an email to the HIA Help Desk notifying completion.

8.0 Track completion of HIA Training

- HIAPPSU updates the HIA Training spreadsheet with completion status.

9.0 Confirm training completion with HIA

- eHS Privacy and Security Lead sends an email to HIA training organizers confirming training completion and updates the OCME User Tracker in SharePoint.

10.0 Notify HIAPPSU about signed Affiliate Acknowledgement

- eHS Privacy and Security Lead informs HIAPPSU via email that Affiliate Acknowledgements are waiting for signature in SharePoint.

11.0 Director signs and stores Affiliate Acknowledgement

- The Director, HIAPPSU, signs the document on behalf of the department and stores the final copy in SharePoint.

12.0 Provide OCME copies of signed documents.

- Upon request, the eHS Privacy and Security Lead provides copies of the signed Affiliate Acknowledgements to OCME.

13.0 Provide eligible user info to eHS training team.

- After training completion and document signing, eHS Privacy and Security Lead provides eligible OCME User info to eHS Training team to start Netcare Training.

14.0 Send URF and SAT Information to eHS OCME mailbox.

- Upon completing Netcare training, OCME User sends the User Registration Form (URF) and Smart Auditing Tool (SAT) info to the eHS OCME mailbox.

15.0 Confirm URF and SAT completion

- eHS Privacy and Security Lead reviews the URF and SAT details, ensures completeness, and forwards to Alberta Health's Netcare Access Administrator (AA).

16.0 Enter SAT info into spreadsheet

- Netcare AA enters SAT details for each CCPP User into a spreadsheet.

17.0 Send spreadsheet to AHS Medical Affairs

- **Netcare AA sends the completed spreadsheet via encrypted email to AHS Medical Affairs.**

18.0 Enter CCPP User info into Application & Privileging (A&P)

- AHS Medical Affairs enters the user info into A&P, which then sends it to AHS LDAP.

19.0 Review and process Netcare/CCPP access

- Netcare AA processes the access credentials through AHS IAM.

20.0 Start Netcare and CCPP access process

- The process follows the established protocols for Netcare, while CCPP access is handled separately by HIAPPSU.

21.0 Create Active Directory (AD) account

- AHS IAM automates the creation of the AD account via the connector to Active Directory.

22.0 Send CCPP role to AHS LDAP

- AHS IAM sends role details to AHS LDAP, which also updates MyLearningLink (MLL) to indicate training requirements.

23.0 Manual steps in Netcare for CCPP Access

- Connect Care Provider IT team adds user context to EMP Managed Access settings.

24.0 Send role to MyLearningLink

- AHS LDAP updates MLL with new role info, enabling access to training.

25.0 CCPP User completes required training

- The user completes the OOB and ECL 200 Introduction to CCPP training via MLL.

26.0 Receive completed training info from MLL

- MLL updates AHS LDAP with completed training records, which are pushed to AHS IAM.

27.0 Provision Netcare/CCPP and AD group, send notification to Netcare AA

- AHS IAM automates provisioning and sends an automated notification to the Netcare Access Administrator (AA).

28.0 Receive AHS IAM notification of CCPP access

- HIAPPSU (AA) receives notification that CCPP access is provisioned, including instructions for Epic Information (Smart Audit Tool).

29.0 Send credential notice to OCME User

- Once access is complete, HIAPPSU sends the credential notice email to the OCME User with cc to eHS Privacy and Security Lead.

30.0 Log into ANP and access CCPP

- The OCME user logs into ANP and accesses CCPP through the "CC Provider Portal" button.

31.0 Confirm successful log-in with OCME

- eHS Privacy and Security confirms with OCME that credentials were received and that the user successfully logged in to CCPP via ANP.

OCME Netcare/CCPP User Offboarding Process

The OCME Netcare/CCPP offboarding process begins when the OCME notifies the eHS Privacy and Security lead to remove access for a specified OCME user. The process involves coordination with various stakeholders, including Alberta Health, AHS IAM, and the Connect Care Provider IT Team to ensure proper removal of the OCME user's Netcare/CCPP access.

Process Flow and Tasks:**1.0 Notification of Offboarding**

- OCME notifies the eHS Privacy and Security lead to remove Netcare/CCPP access for an OCME user.
- The notification must include the OCME user's name, job role, regulated health profession, and office location (Edmonton or Calgary).

2.0 Email Notification to Alberta Health (AA)

- The eHS Privacy and Security lead sends an email to Alberta Health (AA) to request the removal of the OCME user's Netcare/CCPP access.
- The email specifies the user to be offboarded and provides necessary details (name, job role, etc.).

3.0 Submission of ANP Request to AHS IAM

- Alberta Health (AA) submits an ANP request to remove Netcare/CCPP access in the AHS IAM system for the specified OCME user.
- The request will trigger the system to begin the offboarding process.

4.0 Removal of CCPP Template from Epic

- The direct API with Epic removes the CCPP template for the user.
- If this is the last template, the user's account is marked as inactive in Epic.

5.0 Connector Removes CCPP AD Group

- The Active Directory connector removes the OCME user's CCPP AD group.
- If the user only has AD for CCPP access, their AD account will be disabled at this point.

6.0 Work Item Generated for Connect Care IT Team

- A work item is automatically generated for the Connect Care Provider Portal IT Team.
- The IT team removes the CCPP user context from the end user's EMP (Enterprise Managed Profile).
- If the CCPP user is a prescriber, they will also be removed from the Provider Group.

7.0 Automated Notification from AHS IAM

- The AHS IAM system sends an automated notification to Alberta Health (AA), confirming that Netcare/CCPP access has been successfully removed for the OCME user.
- This notification ensures that all relevant parties are informed of the access removal.

8.0 Final Confirmation from AHS IAM

- Alberta Health (AA) receives an automated notification from the AHS IAM system confirming the removal of Netcare/CCPP access for the specified OCME user.

9.0 Update of Encrypted OCME User's Tracker

- The eHS Privacy and Security lead updates the Encrypted OCME User's Tracker, stored in Ensemble, to indicate that the user's access has been deleted.
- This ensures the system reflects the user's offboarding status.

Conclusion

The integration of the Connect Care Provider Portal (CCPP) with the Alberta Netcare Portal (ANP) plays a vital role in enhancing patient continuity of care by providing community providers, their clinical staff, and the Office of the Chief Medical Examiner (OCME) affiliates with secure access to critical health information within the Alberta Electronic Health Record (EHR).

This process ensures that only authorized personnel, governed by strict privacy and security standards, are granted access to the CCPP, maintaining the confidentiality and integrity of patient data. By adhering to the Alberta Health Information Act (HIA), the Alberta Electronic Health Record Regulation, and utilizing the Alberta Health Services (AHS) Identity Access Management (IAM) system, we mitigate risks of unauthorized access while ensuring seamless and secure access to health information.

Regular auditing, monitoring, and vulnerability assessments ensure ongoing compliance and address any potential security concerns, allowing healthcare professionals to deliver optimal care while safeguarding patient privacy. The commitment to following the outlined process is critical in maintaining the trust of all stakeholders involved and in ensuring the continued protection of sensitive health information.

4 Terms, Acronyms, and Abbreviations

Provide a list of the key terms, acronyms, and abbreviations used in this document.

Term/Acronym	Description
AD	Active Directory
AH	Alberta Health
AHS	Alberta Health Services
AHS IAM	Alberta Health Services Identity Access Management
ANP	Alberta Netcare Portal
A&P	Application & Privileging
CA	Coordinating Agent
CCPP	Connect Care Provider Portal
CRF	Custodian Registration Form
CRM	Customer Relationship Management
DSR	Delivery Site Registry
eHS	eHealth Services (CGI)
HIA	Health Information Act
HIAPPSU	HIA Policy, Privacy and Security
LPR	Limited Production Rollout
MLL	My Learning Link
NAA	Netcare Access Administrator
NAR	Network Activation Request
OCME	Office of the Chief Medical Examiner
OIPC	Office of the Information and Privacy Commissioner
OR	Onboarding Request
OU	Organizational Unit
PIA	Privacy Impact Assessment
pORA	Provincial Organizational Readiness Assessment

Term/Acronym	Description
RUNA	Remote User Network Access

5 References

Provide a list of the other documents referenced in this document.

File Name and Location	Description
SharePoint	Amended CCPP Via ANP PIA Endorsement Letter (TBD)
SharePoint	Information Manager Agreement
SharePoint	Information Exchange Protocol
SharePoint	Provincial Organizational Readiness Assessment 2
SharePoint	Connect Care Provider Portal (CCPP) Access Agreement and Epic Addendum
SharePoint	User Registration Form (URF)
SharePoint	OCME Affiliate Acknowledgement

(e.g., Release 2) in the appropriate column.



Connect Care Provider Portal - FAQ

Connect Care Provider Portal Introduction	2
What is Connect Care Provider Portal?	2
What is the difference between Connect Care “Hyperdrive” and Connect Care Provider Portal?	2
Why Use Connect Care Provider Portal?	2
Accessing Patients in Connect Care Provider Portal.....	2
Secure Messaging	3
How and when are patients able to message me?	3
What happens to messages after they have been read?.....	3
How quickly should patient messages be responded to?	3
What is a message pool? Who will see my messages? Who can respond to these messages?.....	3
Can I send a secure text message (SMS) to my patients?	3
MyAHS Connect.....	4
What is MyAHS Connect?	4
Who is eligible for MyAHS Connect?	4
How can MyAHS Connect improve care?	4
What test results can my patients see with MyAHS Connect?	5
What clinical notes can patients see in MyAHS Connect?.....	5
What is Proxy Access?	5
Technical Questions.....	5
Who can I call if I have questions about Connect Care Provider Portal?	5
How do I get access to CCPP for a new provider or staff member at my clinic?	5
How is Netcare connected with Connect Care Provider Portal?	5
Is there a way to connect my clinic’s EMR system with Connect Care Provider Portal?	6

Connect Care Provider Portal Introduction

What is Connect Care Provider Portal?

The Connect Care Provider Portal (CCPP) is an application that is designed for community providers to improve the continuity of care for patients that access services within AHS facilities and are using Connect Care. Components of Connect Care Provider Portal will be available to clinical and administrative staff. Access to clinical information, messaging and viewing of upcoming AHS appointments are some of the tools within CCPP that will enhance the care provided by community users and AHS providers.

What is the difference between Connect Care “Hyperdrive” and Connect Care Provider Portal?

“Hyperdrive” is the complete version of Connect Care that involves establishing a connection through Citrix. During an encounter, Connect Care is used for all aspects of care from referral or patient visit/stay to discharge summary. CCPP provides community providers/staff the ability to see the events of their patient’s encounter.

CCPP is targeted at providers who work primarily external to AHS. Users could include the following:

- Mixed-context providers and their staff
- Contracted community pharmacists
- Contracted continuing care pharmacists
- Continuing care waitlist and vacancy management
- Research monitors

Why Use Connect Care Provider Portal?

Some of the benefits of using CCPP include:

1. Read-only access to a patient’s Connect Care chart:
Lab & DI test results, notes, medications, allergies, letters, referrals, media & care teams
2. Track referrals in Connect Care and upcoming AHS appointments
3. Complete tasks related to a message by clicking context-specific buttons on the toolbar.
4. Communication Between Users:
CCPP users and Connect Care users can use In Basket secure messaging to:
 - Send and receive messages about patient care.
 - Directly link a patients’ chart to messages.

Accessing Patients in Connect Care Provider Portal

CCPP users will have access to patients they have a relationship with as defined by the patient’s care team. If a provider does not have that relationship defined, they have the option to look up a patient based on demographic data (name, sex, date of birth). Connect Care has a real-time interface to AHS Client Registry and should have all patient charts available for lookup if a chart exists.

Secure Messaging

How and when are patients able to message me?

CCPP users will be able to send messages to their patients who have a MyAHS Connect account (please refer to page 4 for information about MyAHS Connect). Patients will be able to send a secure message to someone on their care team if the provider has direct Hypderdrive access.

What happens to messages after they have been read?

Once a staff member reads a message and marks it as “done”, this message goes to their “completed work” folder. Messages from this folder are purged after 60 days.

If a patient messages a provider, this creates an encounter in the patient’s chart and that message is not purged.

How quickly should patient messages be responded to?

Messages should be responded to within 5 calendar days. Messaging is provided to patients informing them that they should not be sending any urgent medical questions to their provider. For urgent issues or questions they are directed to call their clinic, contact Health Link, or go to an emergency department.

What is a message pool? Who will see my messages? Who can respond to these messages?

A “message pool” is a group of people who all receive a single message that requires action from any one person in the group. When one person in the pool completes the task and marks the message as “done”, the message disappears from all other pool members’ In Baskets.

Clinics will have the option to create 3 message pools:

- For physicians
- For clinical staff
- For non-clinical staff (front desk staff)

Incoming patient messages will first be routed to the clinical staff pool. From here a staff member will triage the messages to different pools or different providers as needed: ie route a message to all clinical staff or physicians at a site.

Note: The message pools functionality is not available for all CCPP users.

Can I send a secure text message (SMS) to my patients?

Text messaging between patients and providers is not available. Patients and providers are currently able to communicate through CCPP and MyAHS Connect by using the secure messaging feature.



For more detailed information on In Basket and Secure Messaging please refer to the Connect Care Provider Portal Quick Start Guide.

MyAHS Connect

What is MyAHS Connect?

“MyAHS Connect” is the name of the patient portal that connects patients to Connect Care information services. It offers patients personalized and secure online access to some of their Connect Care health record, communication, care management and health monitoring tools to help them achieve their healthcare goals. Patients can:

- View a summary of their health information and health conditions
- Access test results and investigation reports
- See information about current referrals and their status
- View scheduled appointments and request appointment changes
- Securely communicate with members of their healthcare team
- When flowsheets and questionnaires are ordered by their healthcare team, patients can also
 - Participate in disease management, outcomes tracking and goal refinement
 - Share smartphone and medical device data (Apple Health, Google Fit, Fitbit and Withings compatible devices)

Who is eligible for MyAHS Connect?

To be eligible for MyAHS Connect, patients must be at least 14 years of age and have the following:

- A valid Alberta Driver's License or Alberta Identification card (with a current address)
- Alberta Personal Health Card (Personal Health Number)
- An email account
- Access to a computer, tablet, or other mobile device

To access their MyAHS Connect account, a patient needs to create an Alberta.ca Account and log in to MyHealth Records.

The following groups will be excluded from MyAHS Connect services:

- Out-of-province patients
- Minors under the age of 14
- Any Alberta resident who does not have a valid Alberta-issued driver's license or Alberta issued identification card
- Admitted to or a resident of provincial or federal corrections facilities

How can MyAHS Connect improve care?

Increased patient engagement using MyAHS Connect can improve health outcomes. This alone can improve the clinician's experience. In addition, My AHS Connect offers many opportunities for getting more done with less effort:

- Patients can help keep their problem list, allergies and medication list current and accurate.
- Patient access to test results has been shown to decrease follow-up calls to the healthcare team, while also helping to reduce unnecessary duplicate testing Clinicians can add comments to important results shared through MyAHS Connect.
- Patient access to After Visit Summaries increases adherence to care plans and guidelines.
- Chronic disease management improves when patients can track health outcomes and share them seamlessly with their healthcare team.

- Better informed patients are less likely to make unnecessary emergency room visits.
- Access to secure messaging can decrease the need for some follow-up visits, freeing clinic time for new patients.
- The eCheck-In process allows patients to provide updates about medications, health issues, etc., prior to a scheduled visit. These will be viewable to staff and can be accepted into the chart where appropriate.
- Shared images of wounds and rashes can improve communication about the effects of therapy

What test results can my patients see with MyAHS Connect?

Patients using MyAHS Connect will be able to see a large variety of test results, including laboratory, pathology and diagnostic imaging. Results are released automatically by the system.

What clinical notes can patients see in MyAHS Connect?

Notes are not automatically released to MyAHS Connect. Users with access to Hyperdrive can share one of the following summative notes to patients with an active MyAHS Connect account;

- Consults
- Discharge Summary
- History & Physical
- Progress Notes
- Transfer Note

The decision on whether that note will be released to the patient is made by the prescriber at the time of the note creation, it cannot be released by an individual who did not author the note

What is Proxy Access?

Proxy access is when a MyAHS Connect user has access to view all the health information of someone else, provided by AHS through MyAHS Connect. For more information see [MyAHS Connect Proxy Manual Quick Start Guide](#)

Technical Questions

Who can I call if I have questions about Connect Care Provider Portal?

For technical support questions, call the IT Service Desk at 1-877-311-4300 or send an In Basket message from CCPP. Click the arrow next to **New Message** and select **Customer Service**.

How do I get access to CCPP for a new provider or staff member at my clinic?

Account provisioning for CCPP is managed using [AHS Identity & Access Management](#) (AHS IAM). Please refer to the AHS IAM user guide for step-by-step instructions about how to add/remove access at your clinic.

How is Netcare connected with Connect Care Provider Portal?

You will be able to access CCPP through a link in Netcare that will open CCPP with the current patient context without having to log-in again.

[Is there a way to connect my clinic's EMR system with Connect Care Provider Portal?](#)

Currently, your clinic's EMR and Connect Care Provider Portal are not interfaced.



Connect Care

Connect Care Provider Portal

Quick Start Guide

Connect Care Provider Portal – Quick Start Guide

Getting Started	3
Help and contact information	3
Browser, system, and connection requirements	3
Navigate CCPP	3
Log out.....	4
Update Program Settings	5
Set up your email preferences	5
Change your default login page	6
In Basket Overview	8
Basic Layout	8
View a message	8
Pools.....	9
Search for a message	10
Send a Message	10
Reply to or forward a message	11
Remove a message from In Basket	11
View sent messages.....	12
Provide another person access to your In Basket	13
Grant In Basket access to another person	13
Attach someone's In Basket to yours	13
View another person's In Basket messages	14
Remove another person from having access to your In Basket.....	14
Access a Patient Chart.....	16
Open a patient chart from Patient List.....	16
Search My Patients by name or MRN	16
Add a patient to my Patient List.....	16
Delete a patient from my Patient List	18
Patient Chart Overview	20
Basic Chart Navigation	20
Filter information	20
Chart Review.....	22
Advance Care Planning	22
SnapShot.....	23
Allergies.....	24

Basic allergy information	24
Detailed allergy information	24
Search Chart	25
Medications	26
Patient Care Teams	27
Patient Demographics	28
Flowsheets	29
Upload Documents.....	30
Referrals.....	31
Upcoming Appointments	32
Catalog	33
Community Providers & Staff.....	34
Launching CCPP from ANP	34
CCPP Roles for Community Providers & Staff.....	34
Community Contracted Pharmacist	36
Launching CCPP	36
CCPP Roles for Community Contracted Pharmacists	36
CCPP Continuing Care Roles	37
CCPP Continuing Care Roles	37

Getting Started

Connect Care Provider Portal (CCPP) is a tool that provides real-time web access to patient information, so you can access patients' clinical data and communicate with Alberta Health Services' organizations to provide quality patient care. This guide takes you on an introductory tour of CCPP. The first pages include information to help you get started, such as browser requirements and how to log in. The rest of the guide contains explanations of how to use CCPP.



Your role assignment will determine what parts of CCPP you can access. Screen shots in this guide may not match exactly to what is visible for your role.

Help and contact information

For help using an activity, click .

- If you forget your password or can't log in, call the **IT Service Desk at 1-877-311-4300**.
- For all other issues, send an In Basket message within CCPP. In In Basket, click the arrow next to **New Message** and select **Customer Service**.

Browser, system, and connection requirements

You must use one of the following Internet browsers to access CCPP:

- Apple Safari version 17 or above*
- Microsoft Edge version 118 or above
- Google Chrome version 118 or above
- Mozilla Firefox version 115 or above*

*Some functionality is lost in Safari and Firefox.

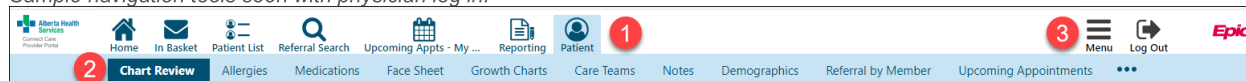
On tablets, you must use iPad Safari or Android Chrome browsers.

CCPP requires a minimum screen resolution of 1024x768 pixels. We recommend that you use a high-speed Internet connection to achieve the best system speed and performance.

Navigate CCPP

When you log in to CCPP, several sets of navigation tools appear at the top of the page. Navigation tools may differ depending on the security access level you have been granted for your specific role.

Sample navigation tools seen with physician log in.




1. **Navigation Tabs:** Use these tabs to open different activities in CCPP. Each tab contains one or more related activities. For example, the **Patient** tab contains patient-specific activities. When you click a tab, the default activity for that tab opens.
2. **Activity Menu:** Use this menu to open the various activities that are contained in the selected navigation tab. For example, the Patient tab activity menu contains several different activities for example, **Chart Review**, **Allergies**, **Medications**, etc.
3. **Action Options:** Use these buttons, located on the top right of the screen, to see all available activities under **Menu** or to **Log Out**.



If there are more activities than can fit on the screen, hover over the ellipsis on the far right of the menu to see all the activities contained in the tab.

Log out

To maintain patient confidentiality, you need to log out or secure your screen when you are done working or have to leave the computer for any reason. There are two ways to do this:

- Click  **Log Out**. The next time you log in, you are directed to your start page.
- Secure the computer by going to **Menu > Secure**. A message will appear indicating that the session is locked and will stay locked for 10 minutes. When you log back in, you will need to enter your password. You will return to the same activity that you were using before you secured the screen.

Update Program Settings

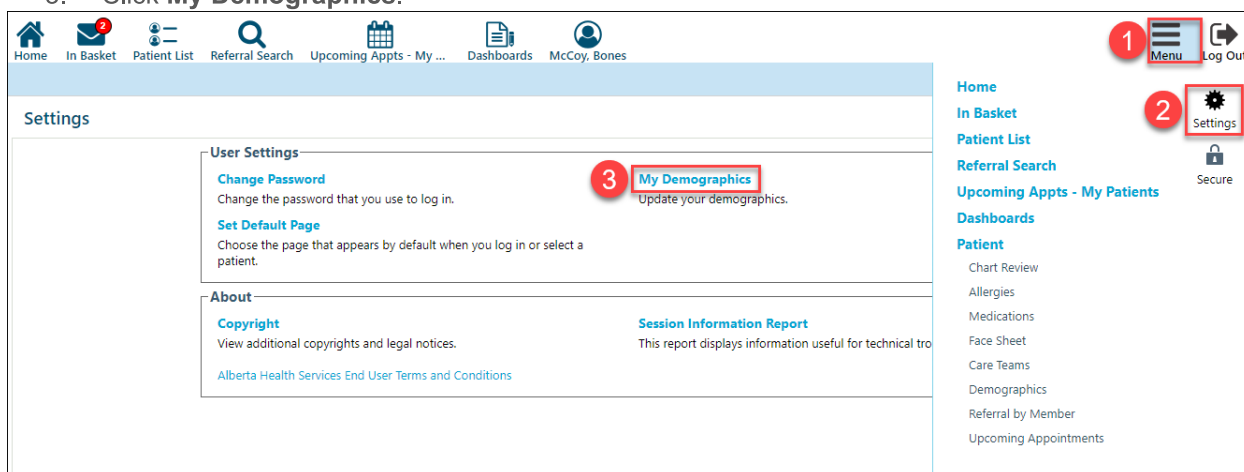
You can use the CCPP settings options to perform a variety of account maintenance tasks, for example, setting your default login page. In addition, you can choose to receive email notifications at an external email address when you are granted access to a patient. You can set your preferences for these notifications, as well as specify the email address at which you'd like to receive them.



You can change settings for other tasks, like determining your default patient selection method. A description of each setting appears on the Settings page in CCPP.

Set up your email preferences

1. Click **Menu**.
2. Click **Settings**.
3. Click **My Demographics**.



4. Update your Email notification settings.
 - a. Enter your **Email**,
 - b. In **Days Between email Notifications**, enter the number of days you want to wait between notification emails.
 - c. In **Notification Preferences**, select the check box beside the notifications you want to receive.
5. Click **Accept**.

Settings > My Demographics

Information

Email a Days Between Email Notifications b

Notification Preferences

☒ Receive email notifications for unread messages ☐ Receive notifications for group events

☐ Receive email notifications when selected for messages in Service Requests ☐ Receive email notifications when not-selected for messages in Service Requests c

Specialties

Family Medicine

Languages

Clinician Title

Degree

MD (will be overwritten by Clinician title)

Addresses/Phone Numbers

+ New Address

Address	Phone	Fax
Royal Alexandra Way Edmonton AB T6E 2J2	780-421-5555	
PO BOX 3955 STN MAIN 4607 50 AVE Olds AB T4H 1P6		

5

Change your default login page

1. Click Menu.
2. Click Settings.
3. Click **Set Default Page**.

Settings

User Settings

[Change Password](#)
Change the password that you use to log in.

[Set Default Page](#) 3
Choose the page that appears by default when you log in or select a patient.

[My Demographics](#)
Update your demographics.

About

[Copyright](#)
View additional copyrights and legal notices.

[Session Information Report](#)
This report displays information useful for technical troubleshooting.

[Alberta Health Services End User Terms and Conditions](#)

Home

In Basket

Patient List

Referral Search

Upcoming Appts - My Patients

Dashboards

Patient

Chart Review

Allergies

Medications

Face Sheet

Care Teams

Demographics

Referral by Member

Upcoming Appointments

1 Menu Log Out

2 Settings Secure

4. Click the tab that you want as your default page.
5. Click **Set Default Page**.

Home In Basket Patient List Referral Search Upcoming Appts - My ... Dashboards Patient **Set Default Page** Menu Log Out

Settings > **Set Default Page**

Set your default page

You can choose the page that appears by default when you log in to Connect Care Provider Portal. If you choose a page which requires a patient to be selected, that activity will also be used as your default page upon selecting a patient. It will also appear when you clear a patient.

To set your default page:

Navigate to the page you want to appear by default and click the Set Default Page button at the top of the screen.

OR

[Click here to clear your default page and use the system settings instead](#)

6. Click **OK**

bld-connectcareproviderportal.albertahealthservices.ca says

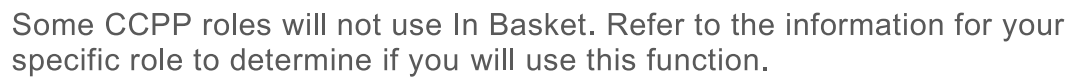
Your start page has been saved.

OK



To reset your default page to the system default, go to Set Default Page and select **Click here to clear your default page and use the system settings instead**.

In Basket Overview



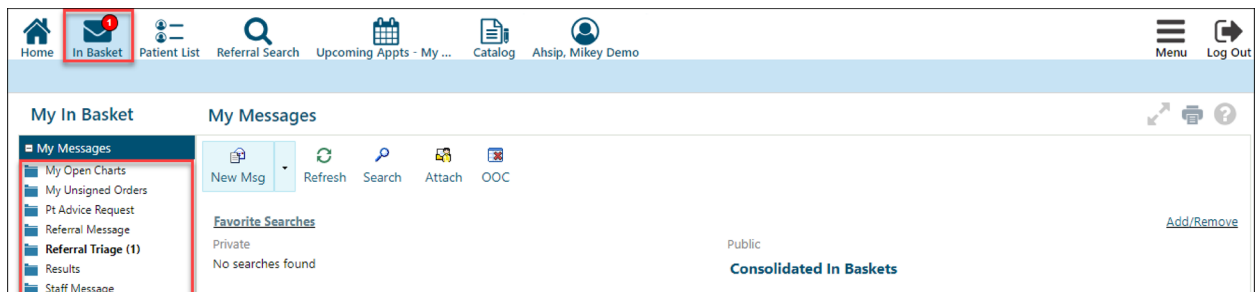
In Basket is a secure, closed, and actionable, task-based messaging system that allows users to manage their daily workflow.



Basic Layout

Click  **In Basket** to access your messages.

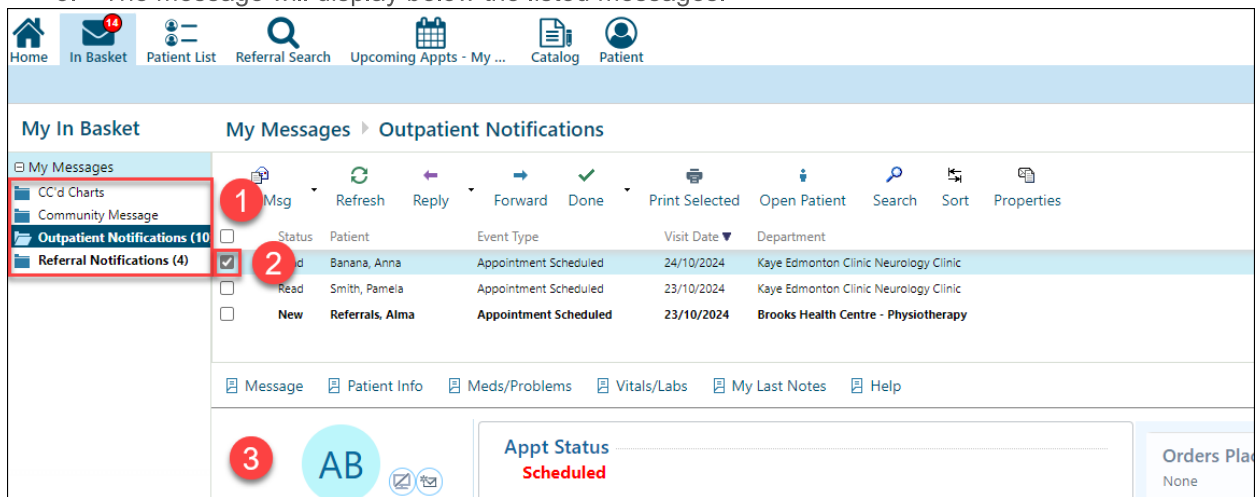
Messages are contained in folders that group types of messages.



If you have new messages, the folder title appears in bold, and the number of new messages appears in parentheses next to the folder name. If you have a new high-priority message, the folder appears with a red arrow.

[View a message](#)

1. Select the folder for the type of message you want to view.
2. Select the check box next to the message you want to view.
3. The message will display below the listed messages.



Pools

In Basket pools are mailing lists that contains a group of users. When a user sends a message to a pool, the message is available to all the members of the pool to view, and any member can act on it.

Messages sent to a pool, are not in a separate folder. To identify a message sent to a pool, look at the **PI** column. If there is an **X** in the column, the message was sent to a pool.

My In Basket		My Messages ▸ Community Message										
<div> <div>My Messages</div> <div>Community File Uploads</div> <div>Community Message</div> </div>		<div> <div>New Msg</div> <div>Refresh</div> <div>Reply</div> <div>Forward</div> <div>Done</div> <div>Open Patient</div> <div>Search</div> <div>Sort</div> <div>Properties</div> </div>										
		Priority ▲		Msg Date	Msg Time	Sent By		Subject	Patient	Action	Phone	PI
				28/10/2024	12:03	PHARMACIST, CONTINUING CARE PROVIDER PORTAL		Testing pool				X

The symbol beside **Msg Date** indicates if anyone is working on the message.

My Messages ▸ Community Message											
<div> <div>New Msg</div> <div>Refresh</div> <div>Reply</div> <div>Forward</div> <div>Done</div> <div>Open Patient</div> <div>Search</div> <div>Sort</div> <div>Properties</div> </div>											
		Priority ▲	Msg Date	Msg Time	Sent By		Subject	Patient	Action		
			28/10/2024	12:03			Testing pool				

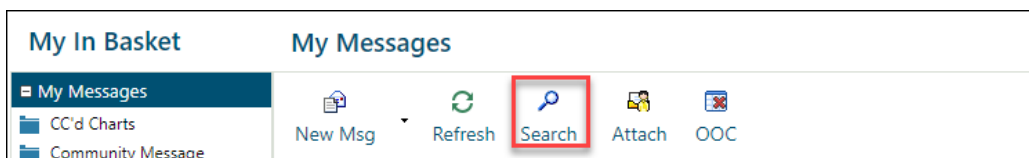
Community Message		
Counts	New	Total
	0	1


Legend		<div> <div>↑</div> <div>↓</div> <div>!!</div> <div>!</div> <div>+!</div> </div> <div> <div>High Priority</div> <div>Low Priority</div> <div>Critical</div> <div>Abnormal</div> <div>Previous Abnormal</div> </div>
		<div> <div>+</div> <div>?</div> <div>-</div> </div> <div> <div>Cc</div> <div>Work Taken By You (Click icon to put back)</div> <div>Work Assigned To Your Pool (Click icon to take)</div> <div>Work Taken By Others (Click icon to take)</div> </div>

If...	Then...
A message has been assigned to your pool but is not being worked on by anyone.	There will be a ? next to the message.
You are working on a message.	Click the ? . It will change to a + to indicate you have taken the message and are working on it.
You took a message but are no longer working on it and it is not complete.	Click the + . It will change to a ? to indicate that the message is not being worked on.
Work on a message is complete.	Click ✓Done . The message is cleared from the In Basket of all recipients. Do not mark a message as done unless all work is complete.
Someone else in the pool has taken the message and is working on it.	There will be a - beside the message.

Search for a message

1. Click  **Search**.



2. Select the search criteria. You can search by In **Baskets**, **Message Types**, **Statuses**, **Message Recipients**, **Priorities**, **Date Message Received**, or any combination of these.
3. Click  **Search**.
4. To return to your normal In Basket view, click **My In Basket**.



Send a Message

Messages can be sent to individual recipients or to multiple recipients grouped in a pool. You can also associate a patient with the message using the **Patient** field on the message form so that the recipient can refer to the patient's chart.

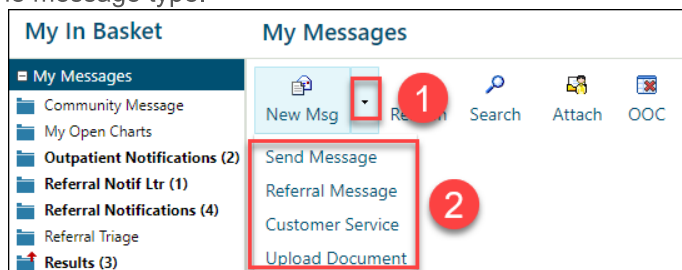
There are 4 message types to choose from:

Message types that you can access will depend on your CCPPP role.


1. **Send Message** – for messages to clinicians using Epic at AHS or AHS affiliate organizations and to other providers using CCPPP. This is the only message type that is **not included** as part of a patient's Epic legal record of care.
2. **Referral message** – for CCPPP users who need to communicate about referrals to an AHS facility.
3. **Customer Service** – for technical support questions
4. **Upload document** – to request that a scanned document be added to a patient's chart in Epic. This message type is not available for all CCPPP roles.


Fields that contain a  are mandatory.

1. Click the  **down arrow** beside  **New Msg.**
2. Select the message type.







3. In the **To** field,


If you are sending the message to individuals	<ul style="list-style-type: none"> • Enter the name of the person you are sending the message to. Press Enter. • To see a list of all recipients, click . <ul style="list-style-type: none"> ◦ Search the list or enter part of the person's name and press Enter.
If you are sending the message to a pool	<ul style="list-style-type: none"> • If you know the name of the pool, enter p, a space, and the pool name (e.g., p AHS ABC). Press Enter. <ul style="list-style-type: none"> ◦ Pool naming convention is Zonal Code + Department Name + Type of Pool (e.g., EDM EEHC FAMILY CARE CL FRONT DESK) • If you don't know the name of the pool, enter p, a space, and ? (e.g., p ?). Press Enter. <ul style="list-style-type: none"> ◦ Search the list or enter p, a space, and part of the pool name and press Enter.

4. Enter a brief subject in the **Subject** field.
5. If you are sending a message regarding a patient, either click **Use <patient name>** to pull in the patient's name, or search for a different patient. This attaches the patient's name to the message.
6. Complete any other required fields.
7. Enter your message in the **Note** field.
8. When you are finished, click  **Send Message**.

Reply to or forward a message

1. Select the folder that contains the message.
2. Select the check box next to the message.
3. To reply to a message, click  **Reply** or click the  **down arrow** beside **Reply** and select  **Reply All**.
4. To forward a message, click  **Forward**.

Remove a message from In Basket

1. Select the folder that contains the message.
2. Select the check box next to the message.
3. Click  **Done**.

The message is cleared from your In Basket.

If a message was sent to a pool, marking is as **Done** will clear the message from the In Basket of all recipients.

If you need to view a message that has been marked as Done, [Search for a message](#) and in **Statuses**, select **Done**.

View sent messages

1. Click **My Sent Messages**.
2. Select the folder that contains the message.
3. Select the check box next to the message.
4. To return to your In Basket, click **My In Basket**.

The screenshot shows the 'My Sent Messages' interface. On the left sidebar, there are three folders: 'Sent Messages' (containing 'Community Message' and 'Staff Message'), 'My In Basket', and 'Attached In Baskets (1)'. The 'Community Message' folder is selected, indicated by a red box and a red circle with the number 2. The main area displays a table of sent messages. The first message is selected, indicated by a red box and a red circle with the number 3. At the bottom of the sidebar, the 'My In Basket' folder is highlighted with a red box and a red circle with the number 4. The 'My Sent Messages' folder is also highlighted with a red box and a red circle with the number 1.

Priority	Msg Date	Msg Time	Sent By	Subject	Patient	Action	Phone	PI
<input checked="" type="checkbox"/>	23/04/2019	14:21	EPICCARE LINK, NURSE	Test	Clover, Richard [1500013956]			X
<input type="checkbox"/>	12/07/2021	07:55	EPICCARE LINK, NURSE	IB Messages				
<input type="checkbox"/>	28/04/2022	14:35	EPICCARE LINK, NURSE	testing				

Provide another person access to your In Basket



Some CCPP roles will not use In Basket. Refer to the information for your specific role to determine if you will use this function.

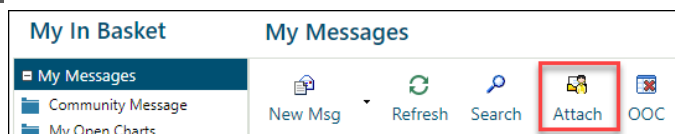
If you want someone else to have access to your In Basket messages:

- You must grant the person access to your In Basket.
- The person you grant access to must attach your In Basket to their In Basket.

There is no way to limit access to your In Basket and the person you grant access to will see all the folders in your In Basket.

Grant In Basket access to another person

1. Click **Attach**.



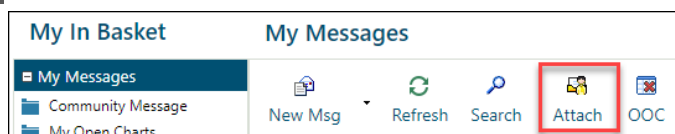
2. Click **Grant Access**.
3. **Grant access to:** Enter the name of the individual who will have permission to access your In Basket and press Enter.
4. The name of the individual will display.
5. Click **Save**.

6. Ensure that the person you granted access attaches their In Basket to yours.

Attach someone's In Basket to yours

After a colleague grants you access to their In Basket, you must attach their In Basket to yours.

1. Click **Attach**.



2. **Add a user to the attach list:** Enter the name of the individual whose In Basket you will have access to, and press Enter.
3. The name of the individual will display.
4. Click **Save**.

View another person's In Basket messages

After you have been granted access and attached another person's In Basket to your In Basket, click **Attached In Baskets** to view another person's In Basket messages.

Remove another person from having access to your In Basket

1. Click **Attach**.

2. Click **Grant Access**.
3. Select the individual you want to remove.
4. Click **Remove**.
5. The name of the individual will be removed from the list.
6. Click **Save**.

In Basket ▸ Grant Access

Attach

Grant Access

 2

Grant the following users access to my In Basket

Grant access to:

3

FAMILY MEDICINE, PHYSICIAN

Remove

 4

← Return to In Basket


✓ Save

 5

Cancel Changes

Access a Patient Chart



Open a patient chart from Patient List

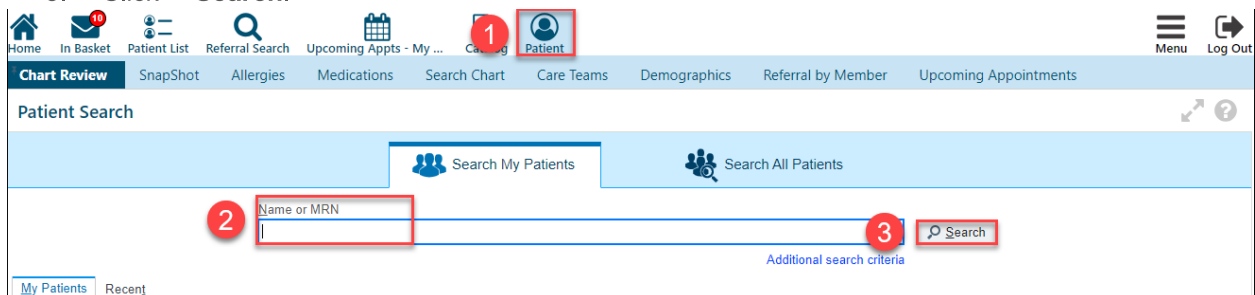
1. Click  **Patient List**.
2. Click a patient's pMRN to open their chart. The patient's name will show in the top navigation field as well as in Patient Storyboard on the left side.
3. To close a patient's chart, click on the "X" beside the patient's name in the top navigation field.



Search My Patients by name or MRN

To find a specific patient from your Patient List

1. Click  **Patient**.
2. Enter the patient's **Name or MRN**.
3. Click  **Search**.



You can quickly open a patient chart that you recently opened. In **Patient Search**, click the **Recent** tab and then double click the pMRN of the patient.

Add a patient to my Patient List



Adding a patient to your Patient List is not available for all CCPP roles. Refer to the information for your specific role to determine if you have access.

If a patient is not on your **Patient List**, you will need to add the patient using **Search All Patients**.

1. Click  **Patient List**.
2. Click **Search All Patients**.

Home In Basket **Patient List** 1 Search Upcoming Appts - My ... Dashboards Patient Menu Log Out

Patient List (5 patient records)

Refresh Filter by PCP:

pMRN	ULI	Patient Name	Date of Birth	Admin Gender	Phone
1000-072-544		Bane, Magnus	08/12/1940	M	555-123-4567
1000-009-363		Cardiology, Carl	10/06/1941	M	608-555-3120

Search All Patients 2

3. Complete all the required fields as noted with the red alert icon.

4. Click Search.

Patient Search

Search My Patients Search All Patients

Fill out the required fields to gain access to a patient/member. Enter additional information for a more accurate match.

Patient Select

Name (Surname, Given name) Sex

Birth date (dd/mm/yyyy) Patient MRN

Search Clear

5. If required, Select the appropriate patient from the displayed list.

6. Select the reason for accessing the patient's chart in the **Reason** field and add any comments in the **Comment** field.

7. Click Select.

McCoy, Leonard "Bones" - 1000022192

Born 05/05/1975 49 y.o. Male 1701 Enterprise way EDMONTON AB T5T 2M8

780-932-3626 (H) Aliases: MCCOY,BONES

Patient Employment

Status Full Time

Reason Comment

Select

8. Once you've accessed the patient's record using **Search All Patients**, the chart will be accessible using the **Patient List**.

Patient List (3 patient records)

Refresh

Filter by PCP:

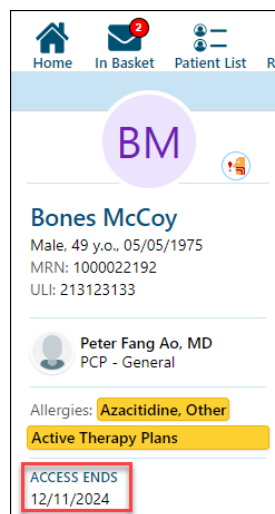
pMRN	ULI	Patient Name	Date of Birth	Admin Gender	Phone
1000-072-544		Bane, Magnus	08/12/1940	M	555-123-4567
1000-009-363		Cardiology, Carl	10/06/1941	M	608-555-3120
1000-022-192	213123133	McCoy, Leonard	05/05/1975	M	780-932-3626

Search All Patients

The length of time you are able to access the patient's chart will depend on your care team relationship.

- If you are not added as part of the patient's Care Team, you will have access to their chart for 60 days. After 60 days, the patient's chart will drop off your My Patients list automatically, and you will need to use the **Search All Patients** list to access the chart.
- If you or someone else adds you to the patient's **Care Team**, you will have ongoing access to the patient's chart.

The date access to the patient's chart will end can be seen on the Patient Storyboard



The Patient Storyboard for Bones McCoy displays the following information:


- Header:** Home, In Basket (2), Patient List, Referred
- Patient Info:** BM (initials), Bones McCoy, Male, 49 y.o., 05/05/1975, MRN: 1000022192, ULI: 213123133
- Provider:** Peter Fang Ao, MD, PCP - General
- Allergies:** Azacitidine, Other
- Active Therapy Plans:** (button)
- Access Ends:** 12/11/2024 (highlighted in a red box)

Delete a patient from my Patient List



Deleting a patient from your Patient List is not available for all CCPP roles. Refer to the information for your specific role to determine if you have access.

If you are no longer part of a patient's Care Team, it is recommended that you remove them from your patient list, so you don't receive any Event Monitor notifications about them.

- Click  **Patient List**.
- Click **Search All Patients**.
- Hover the mouse over the patient and click **X**.

Home In Basket Patient List Referral Search Upcoming Appts - My ... Dashboards McCoy, Bones Menu Log Out

Patient Search

Search My Patients Search All Patients

Name or MRN Search

Additional search criteria

My Patients Recent

Last Accessed	pMRN	ULI	Patient Name	Date of Birth	Admi...	Phone	Street Address
15 mins ago	1000-301-182		AHSCoconnect, Fred	24/02/2000	M	403-111-3333	123 Anywhere str...

3. Confirm that you have the correct patient and click  **Remove Patient.**

Remove Patient

AHSCoconnect, Fred - 1000301182

Born 24/02/2000
24 y.o. Male



123 Anywhere street
CALGARY AB T3R 0V6

403-111-3333 (H)
780-555-1234 (M)

No e-mail address on file

Select the patient groups to remove the patient from:

Your personal patient group

 Remove Patient  Cancel



If you remove a patient in error, you are not able to undo this action. To return a patient to your patient list, perform a Patient Search again.

Patient Chart Overview

Basic Chart Navigation

When you have selected your patient from either the patient list or patient tab, there are a variety of functions available to you to view the patient's healthcare information.

1. The **Patient Storyboard** is always visible while working in the chart to help you quickly find information about the patient including attending physician, date of birth, allergies, etc. More detailed information is available by hovering the cursor over items on the Storyboard.
2. The Activity Menu contains tabs that open different parts of the chart such as Chart Review, Allergies or Medications.
To see all the tabs you can access, hover the cursor over the **More Activities** icon.
3. Under some activities such as **Chart Review** there are tabs that open specific sections of the chart.

Service Date	Note Date	Note Type	Enc Type	Author	Service	Linked Surgery	Enc Department	Sensitive?	Work Type
13/06/2022 14:10	13/06/2022 14:23	Progress Notes	Office Visit	Home Living Nurse A Ccs, RN - Registered Nurse			INTEGRATED HOME CARE (AIRDRIE)	Not Sensitive	
09/05/2022 11:45	09/05/2022 11:42	Progress Notes	Office Visit	Karen Redepinning			INTEGRATED HOME CARE (AIRDRIE)	Not Sensitive	
17/03/2021	17/03/2021	Progress Notes	Orders Only	Attending Physician			Edmonton	Not	

Filter information

You can use filters to find more specific information in the chart.

1. Click the **down arrow** beside **Filters**.
2. Select a filter type. The filters available are specific to the tab that was selected. In this example, Order is selected.

Attachment Type	Authorizing Provider	Department Specialty	Encounter Department	Encounter	Encounter Type	Episode	Ordering Provider	Order
			nine -- Blood			hate, Urine, 2		ol, Urine, 24

3. Select the check boxes next to the values that you want to see. In this example, Creatinine is selected.
4. Click **Apply**.

BM

Bones McCoy
Male, 49 y.o., 05/05/1975
MRN: 1000022192
ULI: 213123133

Search Chart

Change patient

SnapShot **Chart Review** Allergies Medications Search Chart Care Teams Demographics Referral by Member

★ Chart Review - Labs Filters

Order	#Ord	Last Date
<input type="checkbox"/> CORTISOL URINE, 24 HOUR PERFORMABLE	1	01/06/2020
<input checked="" type="checkbox"/> CREATININE	3	28/09/2022
<input type="checkbox"/> CREATININE TOXICOLOGY URINE	8	25/11/2019
<input type="checkbox"/> CREATININE URINE, 24 HOUR PANEL	1	13/04/2020

4

- Click **Start Review** to view the filtered information.
- Click **Clear All Filters** to clear the search criteria.

BM

Bones McCoy
Male, 49 y.o., 05/05/1975
MRN: 1000022192
ULI: 213123133

SnapShot **Chart Review** Allergies Medications Search Chart Care Teams

★ Chart Review - Loaded: 124, Filtered count: 3

Notes Labs Imaging Meds Media Letters Referrals

5 Refresh Filter 6

Filters: Hide Canceled, Order (CREATININE)

Chart Review

Chart Review allows you to open specific areas of the chart.



Different CCPP roles will have access to different areas of the chart. Chart Review tabs will only display if you have access to that part of the chart.

1. Open the patient's chart.
2. Click **Chart Review**.
3. Click the tab for the section of the chart you want to open.
4. Click the link to see additional information.

Magnus Bane
Male, 83 y.o., 08/12/1940
MRN: 1500456239
ULI: No Value Set
Language: English
ACP/GCD: No active order; search

Chart Review - Loaded: 16

Encounters Notes Labs Imaging Cardiology Procedures Surgeries Meds LDAs Media Letters Episodes Referrals

Start Review Refresh Filters

Date Noted	Status	Date Resolved	Type	Episode
19/04/2024	Active		Continuing Care Supportive Living Care	Continuing Care Supportive Living Care

Advance Care Planning


Advance Care Planning and Decision Making Documents that have been added to the patient's chart can be viewed in **Media** tab of **Chart Review**.

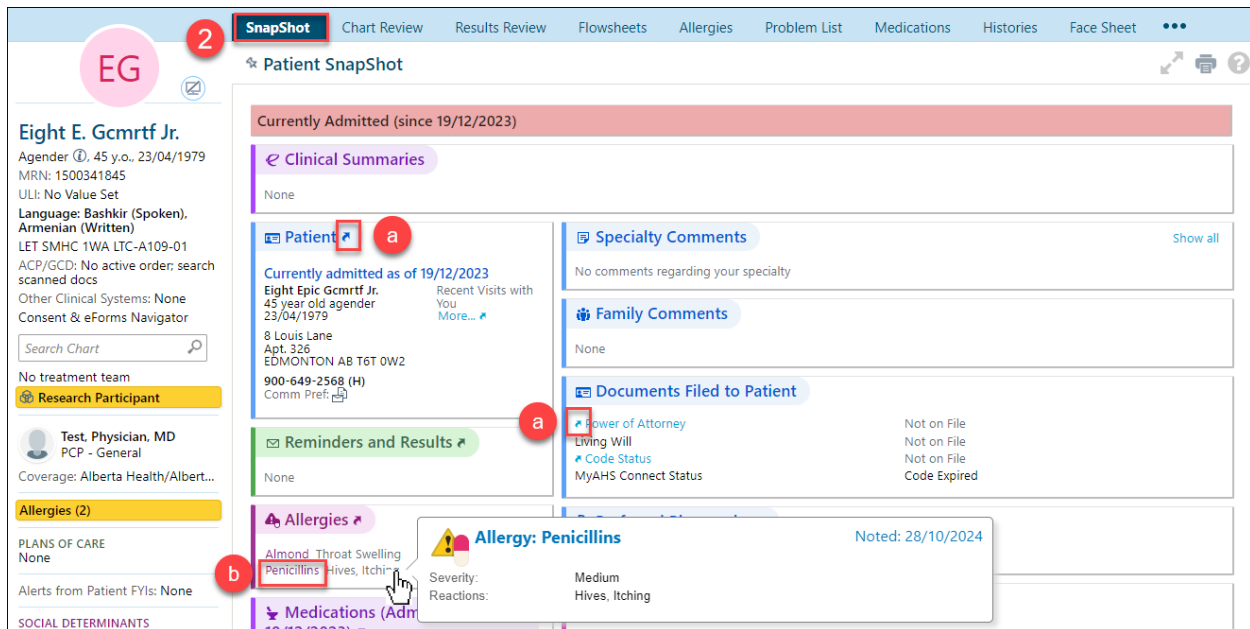
The following is a list of approved Advance Care Planning and Decision Making Documents that can be added to the patient's health record:

- Advance Care Planning Tracking Record
- Capacity Assessment Report
- Decision Making Authority Form
- Enduring Power of Attorney
- Goals of Care Designation Order
- Guardianship Order
- Incapacity/Regained Capacity Declaration
- Jehovah Witness- Refusal of Blood and Blood Products
- Organ & Tissue Donation
- Personal Directive
- Trusteeship Order

SnapShot

SnapShot provides an overview of the patient's chart.

1. Open the patient's chart.
2. Click **SnapShot**.
3. To see more information:
 - a. Click the  **Go To Arrow**.
 - b. Hover the mouse over the text.



The screenshot displays the SnapShot patient chart interface. The top navigation bar includes tabs for SnapShot, Chart Review, Results Review, Flowsheets, Allergies, Problem List, Medications, Histories, and Face Sheet. The patient's name, Eight E. Gcmrtf Jr., is prominently displayed on the left, along with their age, gender, and MRN. The main content area is divided into several sections: Clinical Summaries, Patient Information, Specialty Comments, Family Comments, Documents Filed to Patient, Reminders and Results, Allergies, and Medications. A red circle '2' highlights the SnapShot tab in the top navigation bar. A red circle 'a' highlights the 'Go To Arrow' icon (a small blue arrow) next to the 'Patient' section header. A red circle 'b' highlights the 'Allergies' section header. A tooltip is visible over the 'Allergies' section, showing details for 'Allergy: Penicillins', including severity (Medium) and reactions (Hives, Itching). The tooltip also notes the date 'Noted: 28/10/2024'.

Allergies

Patient allergies can be viewed 2 different ways.

Basic allergy information

1. On the **Patient Storyboard**, hover the mouse over the **Allergies** section.

Chart Review - Loaded: 30, Filtered count: 30

Notes Labs Meds Media Letters Referrals

Start Review Refresh Filters Hide Add'l Notes

Filters: Hide Add'l Notes

Service	Note Date	Note Type	Enc Type	Author	Service	Linked Surgery	Enc Depart
Allergies							
Peanut Oil		High		Reviewed by Community Paramedic on 31/05/2021			
Pollen Extracts		Medium		Hives, Anxiety, Sneezing, Eye Irritation			

Detailed allergy information

1. Open the patient's chart.
2. Click **Allergies**.
3. Click **Past Updates** to view additional information about a specific allergy.
4. Click and select **Deleted** and/or **Expired** to view these allergies.
5. Click **+Add** to add a new allergy. There are search fields to help identify the agent and reactions. There are drop down boxes to fill in reaction type and severity. When addition is complete, click **✓Accept**.



Adding or editing allergy information is not available for all CCPP roles.


Allergies

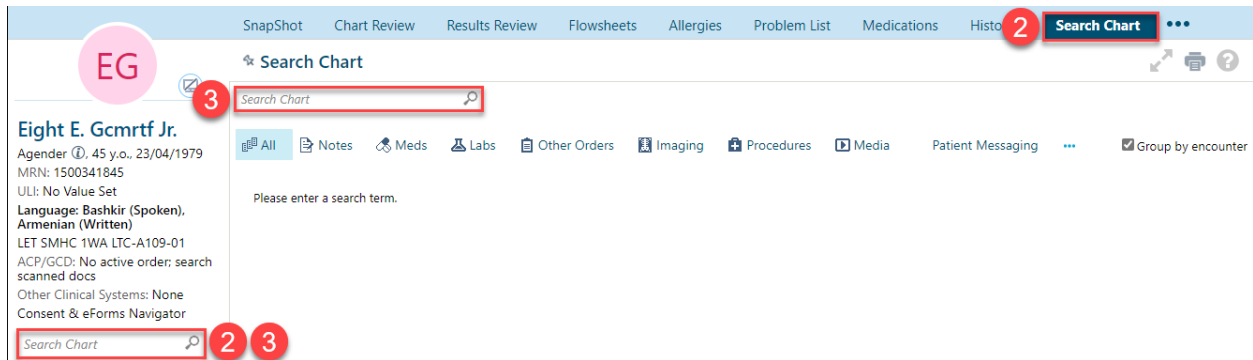
Add a new agent **+ Add** ☐ Full Search

Show: ☐ Deleted ☐ Expired **Choose Columns**

Allergen Types	Reaction	Severity	Reaction Type	Noted	Updated	
Iodine And Iodide Containing Products	Chest Pain	High	Allergy	12/03/2019	Past Updates	
Morphine	Chest Pain	High	Systemic	15/08/2018	Past Updates	
Pineapple	Drug Ingredient, Food	High	Adverse Drug Reaction	26/04/2019	Past Updates	
Strawberry	Drug Ingredient, Food	Anaphylaxis	Systemic	15/08/2018	Past Updates	
Codeine	Drug Ingredient	Dermatitis, Rash	Medium	Topical	15/08/2018	Past Updates
Abatacept	Drug Ingredient	Not Specified		04/09/2019	Past Updates	
Acetone	Drug Ingredient	Not Specified		13/09/2024	Past Updates	

Search Chart

1. Open the patient's chart.
2. Click **Search Chart**.
If the tab is not visible, hover the cursor over the **More Activities** icon.
Option: **Search Chart** is also available on the patient's Storyboard
3. Type the word(s) you want to search for and click .



EG

Snapshot Chart Review Results Review Flowsheets Allergies Problem List Medications History **Search Chart** More Activities

Search Chart

Search Chart

Eight E. Gcmrtf Jr.
Agender ①, 45 y.o., 23/04/1979
MRN: 1500341845
ULI: No Value Set
Language: Bashkir (Spoken),
Armenian (Written)
LET SMHC 1WA LTC-A109-01
ACP/GCD: No active order; search
scanned docs
Other Clinical Systems: None
Consent & eForms Navigator








All Notes Meds Labs Other Orders Imaging Procedures Media Patient Messaging Group by encounter

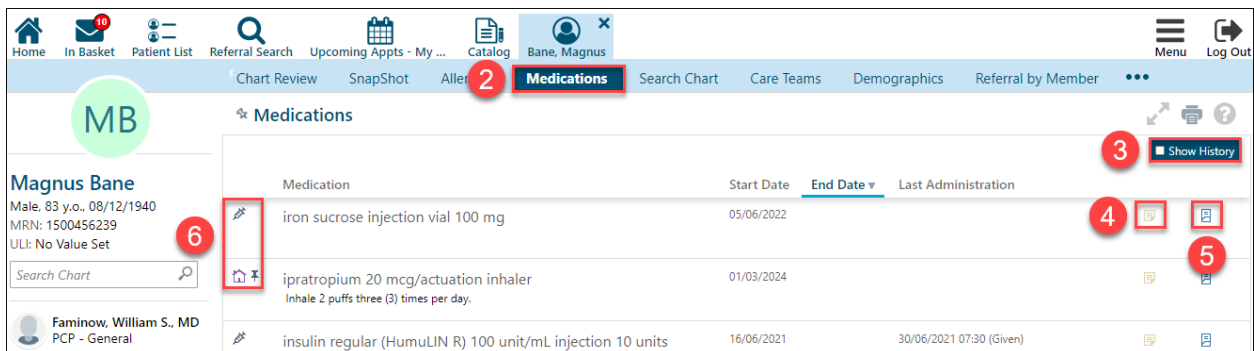
Please enter a search term.

Search Chart




4. All instances where the word appears in the chart will display.
5. Click any instance.

Medications

1. Open the patient's chart.
2. Click **Medications**.
3. Select **Show History** to see medications ordered or documented.
4. Click  **View Notes** to see medication notes.
5. Click  **View Details** to see the order details.
6. Icons provide additional information about the medication:
 -  Long term medication
 -  Hospital medication
 -  Self-reported medication
 -  Prescription
 -  Clinic-administered medication



Medications

Medication	Start Date	End Date	Last Administration
 iron sucrose injection vial 100 mg	05/06/2022		
 ipratropium 20 mcg/actuation inhaler Inhale 2 puffs three (3) times per day.	01/03/2024		
 insulin regular (HumuLIN R) 100 unit/mL injection 10 units	16/06/2021		30/06/2021 07:30 (Given)

Patient Care Teams

To have ongoing access to a patient's chart you must be added to their Care Team. Edits to the Care Team can only be made by mixed-content providers in Hyperspace. Existing Care Teams can be viewed in CCPP.

1. Open the patient's chart.
2. Click **Care Teams**.
If the tab is not visible, hover the cursor over the **More Activities** icon.
3. Click on a **Team Member** to see additional details.

Team Member	Relationship	Specialty	Start Date	End Date
2. Cgy Ach Pulm Func Pft Tech			19/04/2023	
Test, Pcp	PCP - Medical Home		31/01/2022	
Epiccare Link, Physician, MD (Inactive)	PCP - General	General Practice	22/01/2019	



If a community provider has been incorrectly identified as the Primary Care Provider (PCP- General), contact the AHS Solution Centre at 1-877-311-4300 (select option 1, then option 1) to have the provider's name removed from the care team.

In the Patient Care Team, the Primary Provider (CPAR) is accessible for viewing, similar to Netcare. To manage those CPAR attachments that do not appear to be valid, i.e., a Primary Provider (CPAR) needs to be removed, this process must occur at the community EMR where that attachment first took place.

Patient Demographics

1. Open the patient's chart.
2. Click **Demographics**.

If the tab is not visible, hover the cursor over the ●●●More Activities icon.

The screenshot shows the patient portal interface for Bones McCoy. The top navigation bar includes links for Home, In Basket, Patient List, Referral Search, Upcoming Appointments, Dashboards, and a dropdown menu for McCoy, Bones. The Demographics tab is highlighted in the secondary navigation bar. On the left, a patient summary card displays the name Bones McCoy, age 49, sex Male, date of birth 05/05/1975, MRN 1000022192, and ULI 213123133. The main content area shows the Demographics section with a table of basic information.

Basic Demographics					
Name	McCoy, Leonard "Bones"	MRN	1000022192	Sex	Male
Date of Birth	05/05/1975 (49 yrs)	Ethnic Group	N/A	Patient Status	Alive
Sex assigned at birth		Marital Status	N/A	Gender identity	

Flowsheets



Viewing flowsheets is not available for all CCPP roles. Refer to the information for your specific role to determine if you have access.

Flowsheets are used to document patient details such as vitals, assessments, daily care.

1. Open the patient's chart.
 2. Click **Flowsheets**.
 3. Click **+ Add** and select the flowsheet you want to view.
- or

Select the appropriate flowsheet from the recently selected list and click **✓ Accept**.

The screenshot displays the Epic EMR interface for a patient named Eight E. Gcmrtf Jr. The top navigation bar includes 'Home', 'In Basket', 'Patient List', 'External Sites', and 'Gcmrtf, Eight Epic Jr.'. The 'Flowsheets' tab is selected and highlighted with a red box and a red circle with the number 2. Below the navigation bar, the 'Flowsheets' section is visible. On the left, there is a sidebar with patient information, including 'Eight E. Gcmrtf Jr.', 'Agender', '45 y.o.', '23/04/1979', 'MRN: 1500341845', 'ULI: No Value Set', 'Language: Bashkir (Spoken), Armenian (Written)', 'LET SMHC 1WA LTC-A109-01', 'ACP/GCD: No active order: search scanned docs', 'Other Clinical Systems: None', 'Consent & eForms Navigator', 'Search Chart', and 'No treatment team'. The main area shows a 'Select a Flowsheet' dropdown with a red box and a red circle with the number 3. Below the dropdown is a list of available flowsheets: 'Vitals', 'Diabetes', 'Behavioural Safety Plan', 'Vitals with Age-Percentiles', 'Lab Summary', 'Transplant Medications and Labs', 'TRAVEL SCREENING', 'CBC', 'Diabetes Brief', 'MyChart Diabetes Follow-Up', 'Glucose Tracking', and 'Iron Studies'. The 'Accept' button is visible at the bottom right of the list.

Upload Documents



Upload Documents is not available for all CCPP roles. Refer to the information for your specific role to determine if you have access.

Do not use this workflow at this time. More information coming soon.

Referrals



Referral Search is not available for all CCPP roles. Refer to the information for your specific role to determine if you have access.

1. Open the patient's chart.
2. Click **Referral by Member**.
3. **View Option:** **Active Referrals** display. Select **Show All Referrals** if required.
4. Click on the referral ID to see more information about a referral.

Referral by Member

View Option: **Show Active Referrals**

Click on the referral ID to see more information about that referral

Referrals found: 1

ID	Payor	Referred By	Referred To	Status	Start Date	Expiration Date	Creation Date
199001	ALBERTA HEALTH		CGY RGH OPHTHALMOLOGY CL	PEND	06/11/2024	06/11/2029	06/11/2024

5. Click **Add Note/Attachment** to add information. This will appear in the Referral Notes section of the Referral.
6. Click **Referral Message** to send an In Basket message regarding this referral.

Referral by Member ▶ **Referral Details**

Add Note/Attachment **Referral Message**

Referral Referral # 199001

Patient Information

Patient Name	Legal Sex	DOB
Mychart, Allison	Female	16/03/1993

Referral Order

Order
Ambulatory Referral to Ophthalmology (Order # 4971600) on 06/11/2024
[View Encounter](#)

Referred To

Department: CGY RGH OPHTHALMOLOGY CL
Specialty: Ophthalmology

Referred By

Provider: Andrew
Location: AHS PROV PROGRAMS

Procedure Information

Service Details	Modifiers	Provider	Requested	Approved
Procedure REF57 - AMB REFERRAL TO OPHTHALMOLOGY	none		1	1

Appointments

No appointments were found.

Referral Notes Number of Notes: 3

Type	Date	User	Summary	Attachment
Letter	06/11/2024 12:30	Andrew	Auto: 13187-AHS RFL - CONFIRMATION OF RECEIPT LETTER - PROVIDER	-

Upcoming Appointments



Viewing Upcoming Appointments is not available for all CCPP roles. Refer to the information for your specific role to determine if you have access.

The **Upcoming Appointments** report sorts appointments by patients in a particular patient group, if applicable, and then by date and time.

1. Click the **Upcoming Appts** tab.
2. If required, adjust the **From:** or **To:** dates and click **Search**.
3. Your patient's upcoming and canceled/rescheduled appointments in the next 30 days display.

Catalog



Catalog is not available for all CCPP roles. Refer to the information for your specific role to determine if you have access.

More information coming soon.

Community Providers & Staff

CCPP allows community providers & staff view information about their patients from within the AHS record of care. Seamless access to CCPP for community providers is exclusively through the Alberta Netcare (ANP), offering a convenient single point of entry. This allows for an in-context launch to the patient's chart that was opened in Netcare.

Launching CCPP from ANP

The user must first open the patient's record in ANP. From there, click on the **CC Provider Portal** tab within Netcare.

More information about launching CCPP from ANP can be found here: [ANP-Launch-Connect-Care-From-ANP.pdf \(albertanetcare.ca\)](#).

CCPP Roles for Community Providers & Staff

There are three roles for community providers & staff within CCPP.

- **CCPP Clinical 1** (Providers: Physicians, NPs)
- **CCPP Clinical 4** (Registered Professionals: RNs, LPNs, etc.)
- **CCPP Clinical 8** (Non-registered Professionals: MOAs, front-desk staff, etc.)

The CCPP role each user receives is dependent on their current ANP role. The table below lists the CCPP functionality these roles will use.

Available Functionality	Additional Links
In Basket	View a message Pools Search for a message Send a message Reply to or forward a message Remove a message from In Basket View sent messages
Provide another person access to your In Basket	Grant In Basket access to another person Attach someone's In Basket to yours View another person's In Basket messages Remove another person from having access to your In Basket
Access a Patient Chart	Open a patient chart from Patient List Search My Patients by name or MRN Add a patient to my Patient List Delete a patient from my Patient List
Patient Chart overview	Basic chart navigation Filter information

Chart Review	Advance care planning
Snapshot	
Allergies	Basic allergy information Detailed allergy information
Search Chart	
Medications	
Patient Care Teams	
Patient Demographics	
Referrals	
Upcoming Appointments	
Catalog	

Community Contracted Pharmacist

CCPP allows community contracted pharmacists to view information about patients from within the AHS record of care. Only patients that have been assigned to a pharmacist pharmacy pool by a case manager can be viewed. Pharmacists will receive 'view only' access and will not be able to document in the patient record.

Launching CCPP

CCPP can be accessed when connected remotely to the AHS Network using an RSA token

- <https://myapps.albertahealthservices.ca/>

CCPP Roles for Community Contracted Pharmacists

- **CCPP Continuing Care Contracted Pharmacist (under contract)**

The table below lists the CCPP functionality this role will use.

Available Functionality	Additional Links
Access a Patient Chart	Open a patient chart from Patient List Search My Patients by name or MRN
Patient Chart overview	Basic chart navigation Filter information
Chart Review	Advance care planning
Snapshot	
Allergies	Basic allergy information Detailed allergy information
Search Chart	
Medications	
Patient Care Teams	
Patient Demographics	
Flowsheets	
Upload Documents	View uploaded documents

CCPP Continuing Care Roles

CCPP Continuing Care Roles

- CCPP Continuing Care Contracted Pharmacist
- CCPP Continuing Care Waitlist and Vacancy Management

More Information coming soon.