Connect Care Provider Portal via Alberta Netcare Portal

AHS PIA Amendment Reference #622

Information & Privacy Advisor

Suzanne Sutherland

AHS Responsible Affiliate

Victoria E. Lane

Chief Privacy Officer

780-735-1259

Expected Date of Implementation: March 1 2025

Source / Destination Repositories and Their Associated PIAs

Source / Destination Repository	OIPC File Reference #
CCPP via Netcare (AHS File # 2848)	032083
Connect Care Clinical Information System (AHS File 2434) *Alberta Health Services' Connect Care Clinical Information System Privacy Impact Assessment (PIA) was submitted to the Office of the Information & Privacy Commissioner 2019-11-01. An updated PIA (2874) was submitted for review October 30, 2023.*	010239
Alberta Health Services' Organizational Privacy Management Framework (2232)	009600
Alberta Health- Alberta Netcare Portal (ANP) Alberta Netcare Portal Addendum 9 (PIA 2024012)	H3879, 000040, 000034,001800 , 002488, 003083,004953, 013776
Alberta Health Services (AHS) - Netcare Clinical Repositories (NCR) PIA Provincial Health Information Exchange (pHIE) Addendum, was accepted on February 14, 2013.	H51772
Connect Care Provider Portal via Netcare (AHS PIA 2848) submitted November 8, 2023.	032083

Section A – System or Practice Summary

The purpose of this project is to support patient care delivered by community primary care providers by enabling them to access Alberta Health Services (AHS) patient records via the Connect Care Provider Portal (CCPP). Formal consultation with Alberta Health (AH) began mid-2022, and in-context launch of CCPP via the Alberta Netcare Portal (ANP) was approved by Portfolio Committee November 3, 2022. This PIA Amendment pertains to the deployment of Connect Care Provider Portal access to mixed context providers, their clinical staff (non-Alberta Health Services staff), and the Alberta Health affiliate, Office of the Chief Medical Examiner. The project aims to assess the value of the available data in supporting patient continuity of care and to evaluate the capacity requirements for a broader rollout. The amendment includes information specific to changes introduced since the original submission. Sections of the Privacy Impact Assessment (PIA) where no change has occurred have been removed[1].

Project Scope

Access to CCPP via ANP will allow primary care providers at physician offices to view patients' information within the context of the care provided by AHS. The scope of this addendum

[1] Refer to AHS PIA 2848 Connect Care Provider Portal via Netcare (OIPC # 032083).

includes the inclusion of CCPP in the Alberta Electronic Health Record (EHR), the deployment of CCPP access to mixed context providers, their clinical staff, and the Office of the Chief Medical Examiner (OCME).[2]

The project will be implemented in a phased approach. Phase 1 will focus on the evaluation of the utility of CCPP across diverse clinic and staff roles in approx. 20-30 sites for a period of ~ 18 weeks.

The selection process will be initiated via an Expression Of Interest. Clinic Profiles will be assessed for diversity, alignment, and site readiness. Site selection criteria will include:

- Geographic Diversity: Urban, rural, and Indigenous clinics.
- ANP Experience: Both experienced and first-time ANP users.
- Staff Roles: Providers, nurses, NPs, MOAs, administrative staff.
- Specialty Practices: Pediatrics, mental health, internal medicine etc.
- Clinic Readiness: Leadership and staff engagement.

Areas of focus will include:

- Access to Patient Health Information:
  - Comprehensive records: history, diagnostics, medications.
  - Workflow integration and usability.
  - Continuity of care across transitions.
- Onboarding and Training:
  - Implementation protocols, role-based access and support.
  - Hands-on guidance during initial use.
- Broader Deployment Insights:
  - Efficiency of onboarding and resource requirements.
  - User adoption and scalability strategies.

Access to CCPP via ANP will be limited to the following Users in the initial phase:

- Mixed-context providers – Physicians and nurse practitioners who meet the “authorized custodian” eligibility criteria established in section 3 of the Alberta EHR Regulation (AEHRR), and their affiliates (i.e., non-AHS):
- Registered health care professionals - these individuals could include, but are not limited to, registered nurses, licensed practical nurses, and allied care professionals (physical therapists, occupational therapists, respiratory therapists, etc.).
- Non-registered clinical staff – typically are medical office administrative staff (MOA), who perform a wide range of clerical and administrative tasks within the community clinic.

[2] Mixed context providers are individuals who have clinical activity both within AHS and a community clinic.

- Alberta Health OCME AH-Affiliate Users – AH and the OCME have signed a Memorandum of Understanding (MOU) to provide Alberta Netcare access to certain OCME Users in order to access the health information of decedents for the sole purpose of disclosing copied Fatality Inquiries Act (FIA) information to OCME conducting investigations under the FIA[3]. Access is restricted to Medical Examiners and Medical Examiner Investigators.

Authorized Users will have access to CCPP via an embedded launch directly from Netcare. Users must be authorized to use both Netcare and CCPP. Each User-type will be given access to information as appropriate to the ongoing provision of health services and continuing treatment and care, in alignment with specified job duties.

Stakeholders

a. Alberta Health Services

b. Alberta Health

c. Recovery Alberta (RA)[4]

Primary Care Alberta (PCA)[5]

Information Storage and Access

Detailed information about information storage and access is documented in the AHS Connect Care (CC) PIA, section D.[6]

Section B – Organizational Privacy Management

A detailed description of the CCPP via ANP Governance Structure that has facilitated discussions and decisions related to this project is documented in the AHS Connect Care Provider Portal via Netcare PIA (032083) submitted November 8, 2023.

[3] Copied FIA Information means health information regarding decedent individuals accessed via Alberta Netcare that is copied, electronically or otherwise, by an OCME User for the purpose of disclosing to the OCME.

[4] As a result of restructuring of the health system in September 2024 RA became responsible for mental health, addiction, and correctional health (M.O.802/2024).

[5] As a result of restructuring of the health system in January 2025 PCA became responsible for primary care health services (M.O.804/2025).

[6] AHS Connect Care PIA 2848 (010239) was submitted for review October 30, 2023.

Section C – Project Privacy Analysis

Information Listing:

Connect Care (CC) is the legal record of care at AHS facilities where it has been implemented. As such, it keeps a record of all health information collected during the provision of health services provided at AHS facilities. Additional detail is documented in the AHS Connect Care PIA section C(1) and in Appendix 1 of this document.

Information Flow and Diagram[7]

Detailed information and a flow diagram and description of the process flow is documented in the AHS Connect Care Provider Portal via Netcare PIA (032083) submitted November 8, 2023.

Legal Authority and Purpose Table

On Jan 8, 2025, the Minister of Health, by way of a written request, 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 via Alberta Netcare. Alberta Netcare is the provincial Electronic Health Record (EHR), also known as the Alberta EHR. The Minister of Health has requested AHS and RA to make the Connect Care information accessible via the Alberta EHR via CCPP[8]. As a result of the request, CCPP has become a part of the Alberta EHR. Subsequently, AH will make CCPP accessible to authorized custodians[9].

[7] Refer to AH Alberta Netcare Portal and associated addenda 1-9 (H3879, 000040, 000034,001800 , 002488, 003083,004953, 013776)

[8] A written request was provisioned in accordance with section 56.3(6) of the Health Information Act (HIA). See Appendix 2.

[9] AH is the designated information manager of the Alberta EHR. AH will provision access to CCPP to authorized custodians as defined in s. 56.1(b)(ii) of the HIA.

Consent and Expressed Wishes

All Connect Care enhanced confidentiality features, such as private encounters, sensitive notes, and break-the-glass functionality, are equally implemented in the CCPP.[10]

Expressed Wishes

Expressed wish management provides patients with an additional layer of privacy controls. A detailed description is outlined in the AHS CCPP via Netcare PIA (032083).

CCPP and ANP share a common expressed wish flag. Expressed wish requests are synchronized between systems to the specified individuals' records. Un-masking events are logged and reviewed in both systems.

Contracts and Agreements and Information Management Agreements

Detailed information about contracts and agreements is documented in the AHS Connect Care PIA, section C(7).The AH OCME MOU can be viewed in Appendix 1 of the AH Alberta Netcare Portal Addendum 9 (PIA2024012).

Section D – Project Privacy and Security Risk Mitigation

Access Controls

All members of the College of Physicians and Surgeons of the Province of Alberta, such as referring physicians, contracted physicians, and community physicians, are eligible to use CCPP via ANP. As a custodian, a physician can take accountability for and approve access for their support staff, who can then assist them by using CCPP via ANP.

CCPP access roles have limits to their functionality that constrain Users' access to what is appropriate for their job duties[11].

Providers using CCPP can access patients once a relationship is defined by membership on the patient's care team in Connect Care. If a provider does not have that relationship already defined, they have the option to look up a patient but must provide a reason, (recorded for audit purposes) for establishing the relationship.

Access Registration

A formal registration process has been created for all individuals requesting access[12]. The ANP registration process for community custodians and OCME has been modified to incorporate appropriate privacy and security controls to facilitate CCPP access at community clinics. The Alberta Netcare Permission matrix has been updated to add CCPP access. For more information refer to section D1 of the AH Alberta Netcare Portal

[10] AHS masking controls are in accordance with the AHR 56.4(2).

[11] CCPP access aligns with the Netcare Access Matrix. See AH Netcare PIA H3879.

[12] Onboarding and Off-boarding processes for CCPP are compliant with policy and procedure of both Alberta Health and AHS. Registration and deployment of Alberta Netcare access to a community clinic is administered by eHealth Services on behalf of AH. See Appendix 6CCPP via ANP Draft Process Flow and Summary v1.0.

Addendum 9 (PIA2024012). The registration process includes the following activities before access is granted:

1. All CCPP Users must agree to the Connect Care Provider Portal User Terms & Conditions. The Terms require all Users to use the CCPP solely to provide health services and to use health information in a manner limited to the care being provided. CCPP Users must acknowledge that AHS may audit their use of the CCPP.
2. Custodians must agree to the AHS Connect Care Provider Portal Access Agreement. Under this agreement, custodians agree to use the CCPP solely to provide health services to their patients who are also AHS patients. Custodians must agree to meet AHS privacy and security requirements and comply with AHS policies and procedures, including those related to access to and the correction of health information, patient expressed wishes, audit, incident management and investigation.
3. The lead community Custodian – is required to review and endorse both the AHS CCPP and the AH Alberta Netcare Portal PIAs.
4. A custodian assumes the role of the lead custodian and designates an 'authorized approver' (AA) for their community clinic. In this capacity, the AA authorizes other providers and their staff, who are their affiliates under HIA, to use the CCPP in accordance with the portal terms and conditions.

5. Lead Custodians must complete AHS' Privacy and Security Self-Assessment and Certification, which is evaluated for compliance by AHS security personnel. The self assessment requires custodians to:

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

6. Custodians must complete the Expedited PIA for CCPP. This process requires the Lead Custodian to send a PIA endorsement letter to the OIPC stating they understand their responsibilities under the Connect Care PIA and the Portal Access Agreement and that they have completed the Self-Assessment and Certification.

7. Upon completion of the above noted documents the completed access agreement is reviewed, and a decision made to approve or decline access.

8. Additional Users at the clinic may then be onboarded by the AA through the following process:

    A. An individual requesting access completes an access request form and for their Authorized Approver. All individuals requesting access are required to complete the Schedule B of the Access Agreement.[13] The lead custodian of the clinic is required to sign the access agreement.

[13] The Connect Care Provider Portal Access Agreement may be reviewed in the AHS CCPP via Netcare PIA (032083) Appendix 7.

B. The AA reviews the access request and confirms the appropriate access for the individual to perform their role.

C. The Access Authorizer ensures the individual completes all training and orientation related to the use before being granted access.

D. The Access Authorizer reviews the request and determines whether access will be granted. If access is denied, then the Access Authorizer informs the requestor. If access is permitted, then the Access Authorizer sets up the account using AHS Identity Access Management (IAM).

9. The Access Authorizer will annually review all User access rights to ensure that each User has only the access privileges required to perform job tasks.
10. The Access Authorizer shall ensure that User activity is reviewed regularly and that disable dormant accounts. AHS emails the clinic's Access Administrator to inform them if a User has not logged in to the portal in over one hundred days.
11. Three audit reports are required to be reviewed monthly by the AA to verify Users are accessing information in compliance with the CCPP User Agreement. AHS emails the clinic's Access Administrator to remind them of their responsibilities to review audit reports if they have failed to do so within the current month[14].
12. The Access Authorizer upon being informed that a password is suspected of having been compromised or has been compromised shall immediately change the password and report the incident to AHS's IT Information Risk Management and AHS Information & Privacy.
13. A list of Authorized clinics, and all supporting documentation is retained on a secure SharePoint site.

Access to Health Information by Role

Access to Alberta Netcare is managed by AHS Identity Access Management System. AHS IAM is a provincial tool that manages confidential identity information and allows Users to request access to online services and applications, such as ANP and CCPP[15].

AHS IAM system is responsible to:

- Guide or direct Netcare AA to select the appropriate CCPP role based on the User's ANP job role.
- Prevent the selection of a CCPP role if the Netcare role is not eligible for CCPP access. The Netcare AA will be prevented from being able to request CCPP access.

CCPP access is limited to AH Netcare roles clinical 1 and clinical 2. Access restrictions are as follows:

- The Requestor must be a mixed context provider, an affiliate of a mixed context provider (regulated and non-regulated), or an OCME - AH affiliate.

[14] See Appendix 3b.

[15] The Alberta Netcare Permission Matrix has been updated to include CCPP access. The CCPP User Roles and Access Table is available via the Netcare Matrix document. See Appendix 2 Alberta Netcare Permission Matrix Guide and Access Table v1.0. AH Alberta Netcare Portal Addendum 9 (PIA2024012).

- Limited to specific AHS IAM profession roles. The CCPP role determined by AHS IAM profession role[16].

User Roles

User Role	Estimated # of Users in role	Position / Job Title	Information User can Access.
Provider	6,500	Physicians, Nurse Practitioners	• Patient lists where the provider is part of the care team, with full patient search. • Face sheet/demographics (view only) • Notes/Letters/Scanned Media (view only) • Lab Results (view only) • Referral Status (view only) • Care team information (view only) • Medications (view only) • Allergies (view only) • Upcoming appointments (view only) • In-basket messaging (send, read, forward messages in context of patient)
Registered Clinical Professional	6,800 Nurses And Allied Health Professionals	Registered Nurses and Licensed Practical nurses	• Patient lists where the provider is part of the care team, with full patient search. • Face sheet and demographics (view only) • Notes/Letters/Scanned Media (view only) • Lab Results (view only) • Referral Status (view only) • Care team information (view only) • Medications (view only) • Allergies (view only) • Upcoming appointments (view only) • In-basket Messaging (send, read, forward messages in context of patient)
Clinic Support Staff	3,400	Medical Office Assistant	• Limited patient search with ULI plus DOB • Face sheet/demographics (view only) • Notes/Letters/Scanned Media (view only) • Lab Results (view only) • Referral Status (view only) • Care team information (view only) • Medications (view only) • Allergies (view only) • Upcoming appointments (view only) • In-basket Messaging (send, read, forward messages in context of patient)

[16] Alberta Netcare - CCPP Role Mapping is documented in the AH Alberta Netcare Portal Addendum 9 (PIA 2024012).

AHS Connect Care Provider Portal Access

In order to access CCPP from Netcare ANP an Alberta Netcare Portal User must have active accounts for both the Alberta Netcare Portal and CCPP. Detailed information about CCPP access is outlined in the AHS CCPP via Netcare PIA (032083) s.D.

Education and Training[17]

Users must complete privacy training and the 'Introduction to Connect Care Provider Portal' training module prior to gaining access to the CCPP. Completion is monitored by AHS. In addition, training materials are available from the CCPP home screen and can be accessed by Users at any time. Detailed information about education and training is documented in the AHS Connect Care PIA, section B(4).

Privacy and Security Risk Assessment and Mitigation Plans

Assessment of Related Privacy and Security Risks

Additional information about privacy and security risks and mitigation is documented in the AHS Connect Care PIA, section D(2)(3).

Privacy Risk	Description	AHS Mitigation Measures	Policy Reference
Unauthorized access to information in the application from within the internal network	As a result of weak or inadequate access controls, information in the application accessed by other network authenticated Users without a need to know.	• Users must complete mandatory steps before ANP and CCPP access is provisioned. • The Identity & Access Management program monitors access to the CCPP using the same standards as those set for ANP. • A Users account will be deactivated after 180 days of inactivity. • A CCPP AA is required to review all accounts annually. • The CCPP is subject to AHS audit processes. CCPP auditing adheres to the Provincial Logging and Auditing Standard. • AHS Privacy will monitor access events with the AHS SAT Tool and will investigate alerts generated. • Access to CCPP via ANP requires two-factor authentication. • A session will timeout after 10 minutes of inactivity. • Access control mechanisms. See AHS CC PIA s. D.	• Code of Conduct • Code of Conduct • InfoCare: On our Best Behaviours • Info. & Privacy & IT Security Training • Confidentiality and User Agreement • Access to Information (Physical, Electronic, Remote) 1105 • Contractor Requirements for Security and Privacy of Information and Information Technology Resources (1107) • Information Technology Acceptable Use (1109) • Collection, Access, Use, and Disclosure

[17] See Appendix 8 Updated Training Material.

Privacy Risk	Description	AHS Mitigation Measures	Policy Reference
		• Encrypted storage of Users passwords. See AHS CC PIA s. D(2). • User access is removed when no longer required. After 180 days of inactivity CCPP accounts will be terminated. User accounts may be reinstated, but only after the User re-completes applicable on-boarding processes, including mandatory privacy and competency training. • Mandatory reporting of any suspected breaches and security incidents is required for further investigation.	of Information (1112) • Information Classification (1142) • Information Security and Privacy Safeguards (1143) • Monitoring and Auditing of Information Technology Resources (1144) • Philanthropic and Honorific Naming and Recognition (1147) • Identity & Access Mgt. Network Access Request (NAR) procedure • Password Management Standard (ITSC-16-00030) • Encryption Standard (ITSC-12-00300) • AHS Cloud Computing Security Standard • Remote Access Standard • Virus and Malicious Code Penetration Standard (ITSC-10-00410) • Mobile Wireless Devices and Services (1160) • Transmission of Information by Facsimile or Electronic Mail (1113) • Secure Logging Monitoring Standard (ITSC-10-01010)
Lack of program specific training on	Privacy and security of information may be compromised in	• Users are trained prior to being given access to the application. • Completion is monitored by IAM.	• Delegation of Authority and Responsibilities for compliance with

Privacy Risk	Description	AHS Mitigation Measures	Policy Reference
business practices, privacy, and security.	the course of performing business functions if employees are not trained to incorporate security and privacy practices in business processes.		FOIPP and HIA (1108) • Collection, Access, Use, and Disclosure of Information (1112) • Information Security and Privacy Safeguards (1143) • Privacy Protection and Information Access (1177)
More information is collected than it is required to achieve the specific business purpose	The application may be configured to accept more data elements than required for the specific business purpose. Also forms (paper or electronic) used for collecting identifying information may capture more information than required.	• Application is configured to only accept required data. See AHS CC PIA s. D(1). • Forms are designed to only allow the collection of information required for performing job tasks. See AHS CC PIA s. D(1).	• Delegation of Authority and Responsibilities for compliance with FOIPP and HIA (1108) • Collection, Access, Use, and Disclosure of Information (1112) • Information Security and Privacy Safeguards (1143)
Lack of appropriate and adequate logging and auditing capabilities	Lack of appropriate and adequate logging auditing capabilities means inappropriate or unauthorized access to identifiable information cannot be captured. This prevents privacy breaches from being detected and investigated as appropriate logs and log reports may not be available for review.	• Data elements are logged in regard to User access – date and time, view, delete, edit, client ID and/or name, User ID. See AHS CC PIA s. D(3.) • User ID or system/application ID associated with the access. • Name of User or system/application that performs the access. • Role (or profession or occupation) of User who performed the access. • Date of access • Time of access • Actions performed during an access. • Name of facility/organization of access • Display screen number or reference. • Stakeholder unique identifier • Stakeholder name • Audit log reports can be generated. The Lead Custodian or Access Administrator may utilize reports are to determine if the access was	• Information Security and Privacy Safeguards (1143) • Monitoring and Auditing of IT Resources (1144)

Privacy Risk	Description	AHS Mitigation Measures	Policy Reference
		consistent with the assigned role of the authorized User. • Log reports are generated in a format that cannot be modified. See AHS CC PIA s. D(3)	
Lack of proactive auditing of Users' activities	Lack of regular proactive auditing could lead to unauthorized or in appropriate access to identifiable information to go undetected.	• Documented auditing process in place. Auditing of CCPP will be completed by the Lead Custodian. Unauthorized or improper access will be reported for investigation. • AHS conducts vulnerability assessments of key infrastructure components and applications to ensure the confidentiality, integrity, and availability of health information and care for Albertans. • AHS conducts annual security assessments of both the Connect Care and Netcare ANP environments, alternating between in-house and third-party assessments. • Mandatory reporting of any suspected breaches and security incidents is required for further investigation.	• Information Technology Acceptable Use (1109) • Information Security and Privacy Safeguards (1143) • Monitoring and Auditing of IT Resources (1144)
Information unavailability	Information becomes unavailable due to unforeseen circumstances	• Contingency Plan/Business Continuity Plan. See AHS CC PIA s. D(2). • CC data centre failover playbook is available for any such incidents/events. • All core systems and data centers are redundant at the city level with fail over/ duplication in Calgary and Edmonton.	• 1140 Business Continuity Planning for IT (1140 Resources section 2.5) • Change Control for IT Resources (1141 section 1.2)
Improper or lack of information classification	Information is misclassified resulting in too little or too much information. Information is retained longer than necessary.	• Information created through the CCPP is marked as confidential. See AHS CC PIA s. D. • Information is held in accordance with the AHS Records Retention Schedule (AHS Records Code 1133-1262 – Patient/Client Records). Information is retained for a period of 30 years. • See AHS CC PIA s. B. • Disposal Process.	• 1142 Information Classification (1142) • Records Retention Schedule (1133-01)

Privacy Risk	Description	AHS Mitigation Measures	Policy Reference
		- See AHS CC PIA s. B.	
Loss or theft of mobile devices or portable storage medium	Information may become exposed to unauthorized individuals through the loss or theft of a mobile device or portable storage medium.	- Prevention of unauthorized disclosure of information contained on a mobile device or portable storage medium. See AHS CC PIA s. D.	- Mobile Wireless Devices and Services (1160)
Other Related Project Risks			
AHS discloses more health information than is essential to meet the intended purpose via Connect Care Provider Portal		- The CCPP User agreement stipulates that the CCPP may be used only to collect health information required to provide health services to the User's patients that are also AHS patients. - Each CCPP User is given access to health information of patients identified as having a care relationship with the CCPP Users who use break the glass functionality to access other patients' health information are subject to audit.	- Code of Conduct - InfoCare: On our Best Behaviours - Collection, Access, Use & Disclosure of Info. (1112) - Monitoring & Auditing of IT Resources (1144)
AHS discloses health information without consideration of the patient's expressed request to limit disclosure.		- Information subject to enhanced confidentiality in Connect Care is not accessible through the CCPP.	- Code of Conduct - InfoCare: On our Best Behaviours - Confidentiality and User Agreement - Privacy Protection & Information Access (1177) - Collection, Access, Use & Disclosure of Info. #1112) - Information Security & Privacy Safeguards (1143) - Monitoring & Auditing of IT Resources (1144)
AHS cannot enforce its policies and procedures on non-AHS Users.		- Auditing is conducted on the usage on a regular basis. AHS may terminate a CCPP Users access if a facility or User are not abiding by the terms of their agreements with AHS.	- InfoCare: On our Best Behaviours - Confidentiality and User Agreement - Privacy Protection & Information Access (1177)

Privacy Risk	Description	AHS Mitigation Measures	Policy Reference
			• Collection, Access, Use & Disclosure of Info. (1112) • Code of Conduct Information Security & Privacy Safeguards (1143) • Information Technology Acceptable Use (#1109) • Monitoring & Auditing of IT Resources (1144) • Delegation of Authority and Responsibilities for compliance with FOIPP and HIA (1108)

Monitoring of Privacy & Security Controls

- AHS operates CCPP on behalf of AH and is responsible for monitoring and auditing the logs of CCPP, security incidents and mandatory breach reporting.
- System access and User activity in CCPP is electronically monitored, recorded and auditable, which meets the compliance requirements for auditing under HIA. Auditing reports will be used to aid in the investigation of suspected or confirmed privacy breaches by the required party(ies).
- The activity log includes complete information about the patient whose information was accessed. Data elements are logged each time an access and its associated action is performed on a patient's health information and include the following:
- Name of User or system/application that performs the access.
- Role (or profession or occupation) of User who performed the access.
- Date of access.
- Time of access.
- Actions performed during an access.
- Name of facility/organization of access.
- Display screen number or reference.
- Stakeholder unique identifier.
- Stakeholder name

Detailed information about monitoring of privacy and security controls is documented in the AHS Connect Care PIA, section D(3), AHS CPP via ANP PIA file #2848 and the AH ANP PIA and addenda (PIA2024012).

Security Control	Description
Network Protection	Firewalls are setup to filter unauthorized access to and from the AHS network.

Security Control	Description
Information Integrity	Robust process to backup files. In the event of an incident where files are corrupted or becomes unavailable, backup files will be used to retrieve clean data.
Email Gateway Protection	Tools and processes in place to contain malicious emails.
End-Point Protection	Antivirus is installed on window-based workstations and servers. There is a process in place to review required file and folder scanning exceptions particularly for clinical applications and medical devices.
Security of Privileged Accounts	Usernames and password of the high-risk accounts are vaulted, and the password is cycled on each retrieval.
Patching	IT follows a process that identifies, tests, implements and reviews most recent patches. A Patch Committee has been created to oversee this process.
Encryption	All computing devices have full disk encryption.
Physical and Environmental	Critical systems are redundant.
Business Continuity and Disaster Recovery	City level redundancy is in place and is fail over is tested twice a year.
Incident Management	Application Monitoring tools, User Reported Incidents, Infrastructure monitoring tools, Network Monitoring Tools, Endpoint protection monitoring tools.
A security self – assessment	Is completed by all locations / organizations that apply to access CCPP at their location before access is granted. The self – assessment is an assertion and validation that the organization understands and employs security practices.

Repository Logging Capability

The logging capability of CCPP meets the *Alberta Electronic Health Record Regulation 6(1).*[18] All Connect Care User activity is recorded in the EPIC activity log.[19] This includes all Users of 'Hyperdrive' and Users of CCPP. AHS staff, volunteers, physicians, and all staff of affiliate organizations that use Connect Care are included in the activity log.

The activity log includes complete information about the patient whose information was accessed. Data elements are logged each time an access and its associated action is performed on a patient's health information and include the following:

- Name of User or system/application that performs the access.
- Role (or profession or occupation) of User who performed the access.
- Date of access
- Time of access
- Actions performed during an access.
- Name of facility/organization of access
- Display screen number or reference.

[18] Alberta Health Regulation 56.8(5).

[19] Epic Systems is the AHS's Connect Care technology partner.

- Stakeholder unique identifier
- Stakeholder name

Audit Process

All CCPP use is logged monthly and is subject to AHS's privacy and security auditing policies and meets the Provincial Logging and Auditing Standard. CCPP passes audit credentials (Provider ID, Patient ULI & Location ID) bi-directionally between Connect Care and Netcare ANP for integrated sessions.[20]Auditing is a shared responsibility between AHS as the owner of the CCPP, and the Lead Custodian(s) who use the CCPP in their clinics. As the owner and operator of Connect Care, AHS is accountable under HIA for investigations and mandatory breach reporting. Accordingly, AHS is responsible for approving access, monitoring, and auditing the logs of CCPP by all Users and distributing information to the Lead Custodian. The Lead Custodian on behalf of other Custodians at the clinic is also accountable for complying with HIA which includes reporting suspected or confirmed privacy breaches, using audit features in CCPP to aid in the investigation of privacy breaches and meeting mandatory breach reporting requirements. The Lead Custodian can delegate the implementation of their auditing obligations to the Access Administrator for the clinic.

System access and User activity in CCPP is electronically monitored, recorded and auditable, which meets the compliance requirements for auditing under HIA. Auditing reports will be used to aid in the investigation of suspected or confirmed privacy breaches by the required party(ies).

Conclusion

The AHS Privacy Office has reviewed the CCPP via Netcare ANP project including the policies, practices, and procedures in place as well as the flow of information among the partnering organizations; and concluded that by ensuring that contractual and information management responsibilities are clearly documented and managed and adequate information security controls are implemented and monitored, a reasonable and acceptable level of privacy protection will be achieved.

The project team understand and have agreed that any future shifts in scope to the project including changes to governance, data process, privacy legislation/legal authorities, information flows, and security measures will merit advising the AHS Privacy Office and may require the development and submission of a review/addendum of this privacy assessment to the Office of the Information and Privacy Commissioner of Alberta. This privacy assessment may be reviewed periodically to ensure the project's continued compliance with privacy legislation.

[20] Alberta Health Regulation 56.8(h).

Appendix Listing[21]

Document Name
Appendix 1: Information Listing
Appendix 2: a) Letter-Minister of Health b) Ministerial Order
Appendix 3: a) User ANP and CCPP via PIA Endorsement Letter b) AHS Connect Care Provider Portal Access Agreement c) CCPP Privacy & Security Self-Assessment and Certification
Appendix 4: Updated CCPP Role Provisions Matrix
Appendix 5: CCPP via ANP Business Requirements
Appendix 6: CCPP via ANP Process Flow and Summary
Appendix 7: CCPP via ANP Privacy and Security Support Process
Appendix 8: Updated CCPP Training Materials CCPP FAQ and CCPP Quick Start Guide

[21] Note Appendices from the CCPP via Netcare (AHS File # 2848) have been replaced with Appendices in the current Amendment.