Connect Care Provider Portal Privacy and Security Self-Assessment and Certification (Self-Assessment)

Alberta Health Services (AHS) takes the privacy and security of our clinical information systems (CIS) including Connect Care very seriously. The purpose of this Self-Assessment is to provide AHS 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). AHS relies on its InfoCare behaviours to help provide a clear set of expectations for those working in and around AHS personal, health and business information. These are outlined in AHS' Privacy Protection and Information Access Policy, following 'Self-Assessment Certification' on pg 5.

Connect Care is a provincial clinical information system which is under the custodial care of AHS. As a Custodian under the Health Information Act (HIA), AHS has duty to confirm CCPP users have taken reasonable steps to safeguard privacy.

Approach:

Completion of this Self-Assessment is a requirement of the CCPP Access Agreement that Custodians at the Clinic are required to sign prior to their access being granted to the CCPP. The Lead Custodian must complete the following Self-Assessment on behalf of those Custodians. In order for these Custodians and Authorized Staff at the Clinic to be granted access to CCPP, all questions in all six (6) sections must have "yes" as a response. Any negative answer will result in access being denied.

Validation and Review:

The Lead Custodian must submit the completed Self-Assessment to AHS. Once received by AHS, the responses provided for all six sections will be reviewed to ensure the Clinic meets the requirements for access to the CCPP. AHS requires all questions to be answered "yes" for the access to be granted to CCPP.

Suspension or Termination of Access:

AHS reserves the right to terminate or suspend access immediately to CCPP in any or all of the following circumstances:

- A breach of the CCPP Access Agreement
- A breach of privacy legislation
- If incorrect or misleading information was provided in the Self-Assessment or any other documentation required by AHS

Termination or suspension may apply to an entire Clinic or specific user depending on the specific circumstance. In the case of a breach caused by users at a Clinic that had adequate controls in place, AHS will assess any required improvements to the security and privacy controls for the Clinic prior to any reinstatement. In those cases, consideration regarding termination or

suspension of access will be made on a case-by-case basis.

Scored Requirements:

Each question in the following six sections is scored individually with either a yes or no as a response. Please note that a response of "no" to any question means that the Clinic is not CCPP ready and the Lead Custodian should not submit the Self-Assessment unless and until all the questions are answered as "yes".

Note – If a Clinic has begun implementation of the control or has implemented the control with known gaps, the response is still 'no'. The Clinic is required to address the gap and implement the control fully before submitting the Self-Assessment.

The Lead Custodian is certifying if the Clinic achieves the intended control based on their knowledge of the people, processes, and technology in place at their Clinic.

Scoring Guidelines:

The following scale can be used to guide the Clinic

- **NO** = the Clinic has not thought of the control and has not implemented anything
- **YES** = the Clinic has implemented the control fully

Section 1

The Lead Custodian confirms, certifies and asserts on behalf of the Clinic and for the purposes of all of the work environments in which health services are provided (including remote access) that:

#	Question	Yes/ No
1	A Privacy Impact Assessment that reflects HIA requirements (including any recent amendments) and the Clinic's current operations has been submitted to and accepted by the Office of the Information and Privacy Commissioner	
2	All computers and devices used by the Clinic staff (in the Clinic/vendor managed or remote) are kept up-to-date for security patches in accordance with the clinic's patching process. (Note: For vendor supported systems, it is advisable to adhere with the vendor's patch management process)	
3	All computers and devices used by the Clinic staff (in the Clinic or remote) are reasonably protected by anti-malware measures/controls	
4	All computers and devices used by the Clinic staff (in the Clinic or remote) that store Health or Personal Information are protected by disk encryption in accordance with recognized industry best practice to the extent that disk encryption is reasonable or practical under the circumstances. If disk encryption is not reasonable or practical, then the Clinic must be able to demonstrate it uses an alternative method of security having an equivalent level of protection as disk encryption, such as restricting the ability to download or save information on computers and devices that	

	access CCPP	
5	All users that will access CCPP have been provided with the Clinic's security and privacy awareness training and are required to take such training on at least an annual basis (or such frequency as AHS determines is required from time to time)	
6	All users that will access CCPP will be required to take the AHS InfoCare On Our Best Behavior course before getting access to the CCPP	

Section 2

The Clinic has developed and implemented a plan to promote and protect AHS principles around the protection and use of Health Information individually and with those in its employ or under contract for services, including:

#	Question	Yes/No
7	Act on Need: The Clinic has implemented practices that demonstrate the importance of protecting and using Health and Personal Information only when needed to conduct a role. These practices must be followed while using the Clinic devices and while working remotely	
8	Consider Purpose: The Clinic has implemented practices that ensure individuals only use Health Information for the provision of health services and this is the sole purpose for the collecting and providing access to Health Information at the Clinic	
9	Disclosure Mindfully: The Clinic has implemented practices that ensure the disclosure of any information obtained through the CCPP is in accordance with obligations under the HIA	

Section 3:

The Clinic must have implemented a password standard or biometrics that aligns or is consistent with the protections established by the AHS principles for safeguarding information on all computers and mobile devices. In addition to the requirements set out in to Section 1 for ensuring malware protection software is running on all devices, the Clinic must have implemented controls to ensure the following:

#	Question	Yes/No
10	Protection of the devices used by the Clinic staff from theft and accidental disclosure of information	
11	Protection of the passwords and login information required for any fob or other authentication device provided by AHS, and any accounts provided to the Clinic by AHS	
12	Implementation of a biometric password (or) a password standard that includes minimum password length, expiration, password complexity and history	

Section 4:

AHS does not permit access to the CCPP by users who access Health Information for reasons that are not related to the assigned role for which they were provided access. AHS conducts proactive audits and other auditing of the CCPP to review whether users have accessed Health Information in a manner that is inconsistent with their assigned CCPP roles. The Clinic must implement controls to ensure the following:

#	Question	Yes/No
13	Accounts are not shared between users	
14	Clinic users do not “snoop” through patient information and only use the system to access information required to do their jobs	
15	The Clinic has implemented policies to discipline any users found to be in breach of these requirements	

Section 5:

Security and privacy controls are unable to help detect or stop a privacy or security breach if the systems are not managed and reviewed on a continuous basis to look for issues requiring attention. The Clinic should therefore develop and implement a plan to perform the following:

#	Question	Yes/No
16	Regular reviews of all computers, servers, wired & wireless network infrastructure and are performed to look for any issues that could indicate a potential or actual privacy or security breach	
17	Software installations may require the use of privileged/administrative accounts; such accounts are tightly controlled (recommended practice is to have priviledge/administrative accounts separate from the regular user accounts)	
18	Ensure access to applications and networks is centrally managed	

Section 6:

Even with a proper set of privacy and security controls, a privacy or security breach can occur in the Clinic. The Lead Custodian must develop a plan to manage suspected breaches. This plan must include:

#	Question	Yes/No
19	Notifying AHS if suspected incidents/breaches relating to the use of ConnectCare	
20	Cooperating and assisting with AHS during internal investigations as required	
21	Assisting AHS with resolution and recommendations arising from investigations	

Self-Assessment Certification:

I,_____(**Lead Custodian**), a

_____ (describe role in the Clinic/relationship to the

Clinic) of the _____ (insert legal name of Clinic) (**Clinic**)

do hereby represent, warrant, agree and certify the following:

1. I am a Custodian as such term is defined under the *Health Information Act* (Alberta) (**HIA**).

2. I am duly authorized to represent the Clinic for the purposes of this Connect Care Provider Portal (**CCPP**) Privacy and Security Self-Assessment and Certification (**Self-Assessment**).

3. I agree and acknowledge that Alberta Health Services (**AHS**) is relying on the information provided by me in this Self-Assessment for the purposes of granting the users at the Clinic access to the CCPP.

4. I agree and acknowledge that AHS reserves the right to revoke the Clinic's access to the CCPP if AHS becomes aware that the information provided in this Self-Assessment is inaccurate, false or misleading as otherwise stated in this Certification.

5. I agree and acknowledge that AHS has the right at any time following execution of the Self-Assessment and the access agreements by the other Custodian(s) at the Clinic, and upon reasonable notice by AHS, to inspect and audit the Clinic's clinical systems, equipment and facilities to ensure continued compliance with the requirements of this Self-Assessment and the access agreements.

6. I agree and acknowledge that continued access to the CCPP by users at the Clinic is subject to any additional conditions specified by AHS from time-to-time and that these additional conditions must be fulfilled to the satisfaction of AHS within the time frames required by AHS, otherwise access to the CCPP by users at the Clinic may be terminated.

Executed by the undersigned Lead Custodian at the location and on the date stated below.

Clinic Name	
Clinic Address	
Lead Custodian (Print Name)	
Signature	
Date	

Please submit the completed and signed document to connectcare.providerbridge@ahs.ca

Alberta Health Services

POLICY

TITLE
PRIVACY PROTECTION AND INFORMATION ACCESS

SCOPE
Provincial

DOCUMENT #
1177

APPROVAL AUTHORITY
Corporate Services Executive Committee

INITIAL EFFECTIVE DATE
July 18, 2018

SPONSOR
Legal & Privacy

REVISION EFFECTIVE DATE
October 16, 2019

PARENT DOCUMENT TITLE, TYPE AND NUMBER
Not applicable

SCHEDULED REVIEW DATE
October 16, 2022

NOTE: The first appearance of terms in bold in the body of this document (except titles) are defined terms – please refer to the Definitions section.

If you have any questions or comments regarding the information in this document, please contact the Policy & Forms Department at policy@ahs.ca. The Policy & Forms website is the official source of current approved policies, procedures, directives, standards, protocols and guidelines.

OBJECTIVES

- To empower **AHS people** to use their professional judgement while collecting, accessing, using and disclosing **health information**, **personal information**, and **business information**.
- To facilitate AHS people's understanding of AHS policies and legislative requirements for the purposes of their roles and responsibilities, including providing quality health care to Albertans.
- To outline the expected InfoCare behaviours of AHS people on how to handle personal information (which includes personally identifiable data about an individual such as name or address, and also photos or other digital recordings), health information (such as health care number and diagnostic information), and business information (such as briefing notes and policy documents).
- To support AHS' legal obligations, as a public body holding personal information and custodian of health information in order to:
    - establish timely access to health information, personal information and records that are in the care and control of AHS;
    - enable the public's right to access their own information;
    - ensure accuracy of AHS records, and to meet AHS' obligations of public accountability as outlined under the *Freedom of Information and Protection of Privacy Act* (Alberta) (FOIP), the *Health Information Act* (Alberta) (HIA) and all other applicable privacy legislation.

- To promote patients' trust that AHS protects their privacy and fosters open dialogue between patients and care providers.
- To reflect AHS' values focusing on increasing transparency to the public.
- To support all AHS strategies including the *Patient First Strategy, Our People Strategy*, the *Information Management/Information Technology Strategy*, and the *Clinical Health Research, Innovation, and Analytics Strategy*.

PRINCIPLES

Healthcare is delivered in a collaborative team focused environment which requires constant sharing of information. AHS recognizes the importance of collecting, using, retaining, and disclosing information to deliver the best possible care while also respecting the rights of the patients, AHS people, and the public. We all share accountability for the collection, use, disclosure, retention, and safeguarding of health information, personal information, and business information.

All AHS people shall conduct themselves in accordance with the expected InfoCare behaviours and to access AHS resources and training as provided to educate themselves on the protection of health, personal, and business information as applicable to their roles and responsibilities.

APPLICABILITY

Compliance with this document is required by all Alberta Health Services employees, members of the medical and midwifery staffs, Students, Volunteers, and other persons acting on behalf of Alberta Health Services (including contracted service providers as necessary).

ELEMENTS

1. InfoCare Behaviours

1.1 AHS people hold each other accountable and support each other to ensure that we all demonstrate the following behaviours:

a) <u>Act on need</u>

We collect, use, and share only the personal and health information that we require to perform our job duties and responsibilities.

b) <u>Consider purpose</u>

We use and access personal and health information for purposes consistent with its collection or as authorized by law.

c) Safeguard Information

We take reasonable measures to safeguard all health and personal information to meet AHS policies, procedures, standards, protocols, and guidelines.

d) Control multimedia

We recognize that photographs, audio, and video recordings may include personal and health information and are mindful of how we use these media.

e) Manage AHS information

We appreciate and safeguard the value and confidentiality of business information.

f) Speak up

We speak up about any perceived departure (accidental or intentional) from these behaviours with each other, to our leaders, and/or through other AHS mechanisms for reporting.

g) Advocate and learn

We ask questions of our leaders, seek resources, complete training and follow best practices.

h) Disclose mindfully

We exercise professional judgement when disclosing to others to ensure it is acceptable, whether authorized by law or with consent.

i) Provide access

We ensure that our health, personal, and business information is available to the public in a timely manner; in accordance with proper processes to obtain access.

j) Enable sharing

We enable information sharing where appropriate, to contribute to healthcare excellence and patient outcomes.

1.2 We complete any mandatory training and sign the AHS *Confidentiality and User Agreement* when starting as an AHS person and then at least once every three (3) years.

1.3 Where our responsibilities include the development or implementation of programs or systems, the responsible program area shall conduct a Privacy

Impact Assessment with the support of the Information & Privacy Team. That assessment shall be maintained and updated throughout the life of the program or system.

1.4 Where our responsibilities include the use of health, personal, or business information for authorized uses, such as research, education, analytics, or the management of our organization, we shall ensure reasonable measures are taken to safeguard the protection of the information and necessary approvals are in place.

1.5 Where our responsibilities include accessing or using AHS people's information, we only do so for the purposes it was collected, with consent, or as otherwise legally permitted. When we are not sure, we first confirm that we are authorized to access or use it.

2. AHS' Commitments

2.1 AHS is committed to supporting AHS people with meeting expected InfoCare behaviours while recognizing our need to provide health care services to the public. This guidance and support is available through the following means:

a) AHS provides information management and records management policies and procedures to ensure the security of the systems and records where personal and health information are stored and shared. Access to these systems is subject to robust security oversight and is logged for audit purposes.

b) AHS is committed to providing resources and communications pertaining to privacy and confidentiality for AHS people.

c) AHS provides mandatory InfoCare training and other training as required.

d) AHS has an Information & Privacy Team to provide support and guidance to the organization to help AHS meet our obligations around the protection of health, personal, and business information.

e) AHS is responsive when its representatives speak up about possible departures from the InfoCare behaviours and takes action where appropriate.

f) AHS conducts any potential privacy breach investigations in a fair and reasonable manner and in accordance with departmental protocols.

g) AHS ensures that any health or personal information audits are conducted in a reasonable manner that meets legal obligations.

3. Access to AHS Information

3.1 AHS is committed and bound to meet its legal obligations under FOIP and the HIA to provide timely access to information held by AHS to AHS people and the public.

3.2 The public can request information held by AHS through established informal sources and channels such as Communications, Data Analytics, HealthLink, Environmental Public Health, the Health Information Management Department, or AHS Human Resources. AHS encourages the use of these informal processes.

3.3 The public can submit a formal request for information as directed on AHS' website. These formal requests are managed by AHS' Information & Privacy Team and the Health Information Management Department.

3.4 Formal requests can be made to access health information under the HIA, and personal information and/or business information under FOIP.

3.5 Formal requests for personal or health information require the explicit recorded consent of the individual who is the subject of the information, or the individual's **authorized representative**, unless disclosure without consent is authorized by law (see the *Disclosure of Health Information* guide for more information).

3.6 A reasonable fee may be associated with making an information request as outlined by FOIP and the HIA.

3.7 Individuals may also request amendments or corrections to their own health or personal information. In the case of a requested amendment or correction, AHS makes reasonable efforts to confirm the accuracy of the AHS records while reserving the right to restrict or decline to make amendments to AHS records.

4. Compliance

4.1 AHS people are required to comply with the InfoCare behaviours.

4.2 AHS is committed to timely and just processes and, if disciplinary action is required, follows the *Progressive Discipline* Procedure and applicable collective agreements to address incidents of unsatisfactory conduct or performance.

4.3 Failure to comply with this Policy may result in disciplinary action up to and including termination of employment or appointment.

DEFINITIONS

AHS people means Alberta Health Services employees, members of the medical and midwifery staffs, Students, Volunteers, and other persons acting on behalf of AHS (including contracted service providers as necessary).

Authorized representative means a person who has been granted legal authority to make decisions on behalf of another person, has written authorization to act on that person's behalf, or is otherwise authorized by law to act on behalf of that person.

Business information means general information, which is any recorded information about AHS' business activities such as those related to facilities, infrastructure, and security; policies and programs; budgets, expenses, and contracts; reports and statistics, etc., that are under the custody or control of AHS.

Health information means one or both of the following:

a) diagnostic, treatment and care information; and
b) registration information (e.g., demographics, residency, health services eligibility, or billing).

Personal information means recorded information, not governed by the *Health Information Act* (Alberta), of any kind stored in any format that identifies an individual including, but not limited to:

a) address and contact information (including an identifying number or symbol assigned to an individual);
b) race, ethnic origin, gender or marital status;
c) educational, financial, employment or criminal history;
d) opinions of others about the person;
e) the image of a person on a photograph; and
f) personal views and opinions of a person (except if these are about another person).

REFERENCES

- Alberta Health Services Governance Documents:
  - *Access to Information (Physical, Electronic, Remote)* Policy (#1105)
  - *Code of Conduct*
  - *Collection, Access, Use and Disclosure of Information* Policy (#1112)
  - *Contractor Requirements for Security and Privacy of Information and Information Technology Resources* Policy (#1107)
  - *Delegation of Authority & Responsibilities for Compliance with FOIP & the HIA* Policy (#1108)
  - *Individually Identifying Information* (#1174)
  - *Information Security & Privacy Safeguards* Policy (#1143)
  - *Information Technology Acceptable Use* Policy (#1109)
  - *Monitoring and Auditing of IT Resources* Policy (#1144)
  - *Privacy Impact Assessments* Policy (#1145)
  - *Progressive Discipline* Procedure (#1116-05)
  - *Research Information Management* Policy (#1146)
- Alberta Health Services Forms:
  - *Confidentiality and User Agreement* Form (#07922)
  - *Consent to Disclose Health Information* Form (#18028)

  - *Consent to collection and use of a recording device or camera for Photographs, Video or Sound Recordings for Health Care purposes* Form (#07998)
  - *Consent To Collect, Use, and Disclose Stories, Photos and/or Video and Sound Recordings* Form (#18273)
  - *Privacy Breach Notification* Form (#09579)
- Alberta Health Services Resources:
  - Access & Disclosure (Health Information Management): disclosure@ahs.ca
  - *Clinical Health Research, Innovation, and Analytics Strategy*
  - Information and Privacy: privacy@ahs.ca
  - *Information Management/Information Technology Strategy*
  - *Our People Strategy*
  - *Patient First Strategy*
  - Whistleblower Line (Confidential): 1-800-661-9675
- Non-Alberta Health Services Documents:
  - *Freedom of Information and Protection of Privacy Act* (Alberta)
  - *Health Information Act* (Alberta)

VERSION HISTORY

Date	Action Taken
October 16, 2019	Revised
Click here to enter a date	Optional: Choose an item