# Table of Content

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose of Guide</td>
<td>3</td>
</tr>
<tr>
<td>Alberta Netcare</td>
<td>3</td>
</tr>
<tr>
<td>Authorized Custodian</td>
<td>3</td>
</tr>
<tr>
<td>Appointing the Alberta Netcare Access Administrator (AA)</td>
<td>3</td>
</tr>
<tr>
<td>User Access Management</td>
<td>4</td>
</tr>
<tr>
<td>Information Security Awareness</td>
<td>5</td>
</tr>
<tr>
<td>Privacy Awareness</td>
<td>7</td>
</tr>
<tr>
<td>Reporting of Breaches</td>
<td>7</td>
</tr>
<tr>
<td>Purpose of the Alberta Netcare Access Administrator (AA) Form</td>
<td>8</td>
</tr>
<tr>
<td>Completion of the Alberta Netcare AA Form</td>
<td>8</td>
</tr>
<tr>
<td>Submission Instructions for the AA Form</td>
<td>8</td>
</tr>
<tr>
<td>Purpose of the Alberta Netcare User Registration Form (URF)</td>
<td>8</td>
</tr>
<tr>
<td>Completion of the Alberta Netcare URF</td>
<td>8</td>
</tr>
<tr>
<td>Remote Access</td>
<td>9</td>
</tr>
<tr>
<td>Alberta Netcare Permission Matrix and Role Assignments</td>
<td>10</td>
</tr>
<tr>
<td>Linked Documents and Items</td>
<td>10</td>
</tr>
<tr>
<td>Alberta Netcare Access Administrator Guide Versions</td>
<td>10</td>
</tr>
<tr>
<td>Access Level Selection Flow Diagrams</td>
<td>12</td>
</tr>
</tbody>
</table>
Purpose of Guide

This guide provides Alberta Netcare Access Administrator’s (AA’s) with instructions to carry out Alberta Netcare User Access Management duties as per the requirements identified in the Alberta Netcare Information Exchange Protocol (IEP) section 6.1. The IEP contains the rules that all authorized custodians and their affiliates must follow with respect to access, use, disclosure and retention of prescribed health information via Alberta Netcare. The IEP is provided to the custodian once they have completed a series of privacy and security assessments to become ‘authorized’ custodians.

Alberta Netcare

The Health Information Act (HIA) defines Alberta Netcare as “the integrated electronic health information system established to provide shared access by authorized custodians to prescribed health information in a secure environment as may be further defined or described in the regulations” (section 56.1(a)). Alberta Netcare is a clinical health information network that links community physicians, pharmacists, hospitals, home care and other authorized custodians across the province. Alberta Netcare does not provide access to a patient’s full record of the health care information.

For more information regarding Alberta Netcare, please visit the Alberta Netcare public website: http://albertanetcare.ca/WhyEHR.htm

Authorized Custodian

Only authorized custodians and their affiliates may access health information in Alberta Netcare. Section 3 of the Alberta Electronic Health Record Regulation provides the requirements that must be met to become an authorized custodian that include:

- the acceptance of a Privacy Impact Assessment (PIA), by the Office of the Information and Privacy Commissioner (OIPC); that identifies and addresses potential privacy risks that may occur at the custodian’s facility;
- the approval of a Provincial Organizational Readiness Assessment (PORA), by Alberta Health; that ensures the custodian facility meets mandatory security requirements; and
- the signing of an Information Manager Agreement (IMA) with Alberta Health, that commits the custodian and their affiliates to follow the rules for accessing Alberta Netcare.

For more information regarding access to Alberta Netcare, please visit the Alberta Netcare Learning Centre website: http://albertanetcare.ca/Registration.htm.

Appointing the Alberta Netcare Access Administrator (AA)

The authorized custodian must appoint an Alberta Netcare AA in order to carry out user access management duties. The authorized custodian appoints the AA by completing the Alberta Netcare Access Administrator (AA) Registration Form.

The appointed AA will act on behalf of the authorized custodian to ensure that affiliate ("user") access to Alberta Netcare information is restricted based on their role in the health care
system. Netcare access should only be set-up to allow users to access enough information to do their jobs, while adhering to the HIA principle of a "need-to-know" basis. The following defines who the AA is for each facility type:

- **Community Facilities** - The AA’s can be the custodian (e.g. physician, pharmacist) or an appointed/delegated affiliate responsible for liaising between the custodian(s) and Alberta Health.
- **Alberta Health Services (AHS) Facilities** - The AA’s are AHS affiliates that are approved by the AHS Executive Director, IT Security & Compliance.
- **Alberta Health Facilities** - The AA’s are Alberta Health affiliates that are approved by the Alberta Health Chief Information Officer.

### User Access Management

The Alberta Netcare AA is the primary contact regarding user access to Alberta Netcare from their facility or facilities. The main responsibility of the Alberta Netcare AA is to perform user access management duties that include the following:

1. **Alberta Netcare Access** - The AA is responsible to ensure that the user’s access to Netcare is based on the HIA principle of a “need to know” and the “least amount of information” to do their job. Specific responsibilities are:
   - Assist affiliates in gaining access to Alberta Netcare by completing the Alberta Netcare User Registration Form (URF).
   - Re-validate user access yearly, to ensure access is correct and is still required. Terminate user access when it is no longer required.
   - Monitor user access to ensure they are adhering to their HIA obligations and the rules for access Alberta Netcare.
   - Review user’s access information and ensure it is accurate and complete. Update as applicable by completing the Alberta Netcare URF.
   - Comply with legislative and custodian policy obligations when collecting user information while performing Alberta Netcare User Access Management duties.

2. **Privacy and Security Training** - Custodians are responsible for the actions of their affiliates. If an affiliate does something HIA forbids them to do, it is as if the custodian did it. Consequently affiliates must comply with HIA, as well as with the policies and procedures adopted by the custodian. As the appointed representative of the custodian, the AA must do the following:
   - Ensure affiliates are aware of their obligations and requirements when accessing Alberta Netcare.
   - Ensure affiliates understand that a person, who knowingly collects, uses or discloses health information in contravention with the HIA may be found guilty of an offence and liable to a fine as defined in that legislation.
   - Inform users that Alberta Health monitors access to Alberta Netcare for security purposes and to protect the information. By accessing Alberta Netcare users are expressly consenting to these monitoring activities.
   - Educate users about what is considered a security or privacy breach and how to report them.
3. **Reporting Security or Privacy Breaches** - An information security or privacy breach occurs when there is a violation of the: HIA; rules for accessing Alberta Netcare information; or security or privacy policies of the custodian. A breach can also happen if there is a failure or absence of required safeguards to prevent a loss of confidentiality, integrity or availability of information. Examples of security incidents include:

- Deliberate misuse of health information in Alberta Netcare.
- A missing laptop, PDA or portable storage device containing health information.
- Virus, spyware or malware infection impacting health information.
- Disclosure of your Alberta Netcare password or other authentication credential.

The HIA has established fines for anyone who knowingly collects, uses, or discloses health information or who gains or attempts to gain access to health information in contravention of the HIA. Individuals who breach privacy and access rules could be subject to criminal charges, fines, and disciplinary measures within their licensing or professional organizations. Consequently the AA must:

- Report information security or privacy breaches promptly as per the defined breach reporting process to ensure that incidents are managed properly in order to isolate and minimize the effects of an adverse event.
- Assist in investigation of potential information security or privacy breaches in Alberta Netcare.
- Act as a liaison between Alberta Health and the custodian to report and provide status updates on incidents.

4. **Auditing User Access to Alberta Netcare** – Custodians are responsible and obligated to protect the privacy and confidentiality of Alberta Netcare information. Access logs play an important role in auditing user access, proactive monitoring and responding to breach investigations. The AA can contact HIA Help Desk at 780-427-8089 or email HIAHelpDesk@gov.ab.ca; or email AH.security@gov.ab.ca to request Alberta Netcare access logs on their users. Alberta Health will contact the AA to obtain the required details, such as the full name of the user and time period; in order to provide the specific access log to the custodian.

Further information on the Netcare AA responsibilities can be obtained via the Netcare Learning Centre: [http://www.albertanetcare.ca/LearningCentre/Access-Admin.htm](http://www.albertanetcare.ca/LearningCentre/Access-Admin.htm).

**Information Security Awareness**

Information security means:

- Preserving the confidentiality and integrity of information and ensuring that the systems are available to provide service to patients.
- Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

The HIA requires custodians and their affiliates to protect health information in their custody or under their control. The Act provides specific requirements for protecting electronic health information.

---

1 Further information on breaches can be found in the ‘Reporting of Breaches’ section of this guide.
records. Custodians must take reasonable steps to maintain administrative, technical and physical safeguards to protect health information. These safeguards are meant to:

- protect both the confidentiality of the information and the privacy of the individuals who are the subjects of that information;
- protect against reasonably anticipated threats or hazards to the security or integrity of health information or the loss, unauthorized access, use, disclosure or modification of health information;
- ensure compliance with HIA and the custodian’s privacy and security policies.

Alberta Netcare AAs assist by safeguarding the confidentiality, integrity and availability of the health information under the control of the custodian. Protecting the confidentiality of information means only authorized users can access sensitive information. Safeguarding the integrity of information is about maintaining the reliability and accuracy of information so it can be used to make informed health decisions. For example an unauthorized change of health information used for decision making or an error in the information is something that causes a loss of integrity to the information. Ensuring the continued availability of information means it is accessible to those who need the information. A system outage is something that causes a loss of availability.

Alberta Health has adopted the Government of Alberta Information Security Classification structure that describes four classification levels of information sensitivity. All health information is classified as confidential.

- **Unrestricted** information is not sensitive and includes information that can be routinely shared with the public.
- **Protected** information is considered sensitive and is not publically available. However it is usually available to all staff.
- **Confidential** information is sensitive information that is not shared with all staff but is only accessible by staff in specific functions or roles.
- **Restricted** information is highly sensitive and only accessible by a limited number of specific staff.

When granting access to Alberta Netcare the following HIA security principles should be followed:

- The **segregation of duties** means the separation of duties in order to manage conflict of interest, the appearance of conflict of interest, and fraud. It restricts the amount of power held by any one individual. It puts a barrier in place to prevent fraud that may be perpetrated by one individual. For example users can not approve their own access to Alberta Netcare it must be approved by the AA.
- The **authorization to use and disclose** means once you have been given access to Alberta Netcare information, you are required to use that information only during the course of your work. Using or disclosing that information for personal gain or for purposes outside of the HIA is prohibited and is considered a breach. The HIA sets out fines for custodians and affiliates who knowingly breach the Act.
Privacy Awareness

The following HIA privacy provisions must be adhered to when granting access to Alberta Netcare. Since the Netcare AA acts on behalf of the authorized custodian it is their responsibility to ensure these privacy provisions are adhered to:

- The duty of a custodian to collect, use or disclose individually identifying health information with the highest degree of anonymity possible (section 57).
- The duty of a custodian to collect, use or disclose the least amount of individually identifying health information (section 58).
- The duty of an affiliate to collect, use or disclose health information in a manner that is in accordance with the affiliate’s responsibilities as determined by their custodian (need to know basis) (sections 24, 28, 43).
- The duty of a custodian to protect the confidentiality of health information (section 60).
- The duty of a custodian to consider the expressed wishes of an individual regarding the disclosure of individually identifying health information (section 58(2)).

Further information regarding the HIA can be obtained from the following:

- HIA Guideline and Practices Manual - provides supplementary information regarding the HIA and Regulations. The Manual explains roles and responsibilities with respect to the administration of the Act, and is intended to provide guidelines and suggest best practices, not binding rules. It also takes into consideration significant decisions of the Information and Privacy Commissioner.
- HIA and Regulations - [http://www.health.alberta.ca/about/health-legislation.html](http://www.health.alberta.ca/about/health-legislation.html)
- HIA Helpdesk can be contacted between 8:15 a.m. to 4:30 p.m. (Monday to Friday, excluding statutory holidays) at:
  - Local: 780-427-8089
  - Toll Free in Alberta by dialing 310-0000 then 780-427-8089
  - Email: hiahelpdesk@gov.ab.ca

Reporting of Breaches

The Provincial Reportable Incident Response Process (PRIRP) will be followed when reporting suspected security and privacy incidents. The PRIRP has been designed to ensure that all health stakeholders such as community custodians, AHS and health service partners are appropriately involved to respond to a suspected or real threat. All suspected breaches for Alberta Netcare must be reported using the PRIRP form. The PRIRP process guide and form are available via the Alberta Netcare Learning Centre - [http://www.albertanetcare.ca/1187.htm](http://www.albertanetcare.ca/1187.htm)
Contact information for questions or the reporting of breaches:

- Alberta Health Customer Service Centre
  - Toll-Free: 1-877-931-1638
  - Phone: 780-412-6778

- Alberta Health Security Team
  - 780-643-9343
  - Email: HIABreachReporting@gov.ab.ca

- Email the completed PRIRP to HIABreachReporting@gov.ab.ca

**Purpose of the Alberta Netcare Access Administrator (AA) Form**

The Alberta Netcare Access Administrator Registration form is used by the authorized custodian (or multiple custodians) to add, remove or amend the Netcare AA for their facility or multiple facilities.

The eHealth Support Consultant can provide more assistance, if required. Contact information is available from the Alberta Netcare public website: [http://www.albertanetcare.ca/contact.htm](http://www.albertanetcare.ca/contact.htm).

**Completion of the Alberta Netcare AA Form**

The most current version of the AA form, guide and other information is available through the Netcare Learning Centre: [http://www.albertanetcare.ca/1187.htm](http://www.albertanetcare.ca/1187.htm).

**Submission Instructions for the AA Form**

Community Facilities (for example: physician offices, pharmacies) - Fax completed forms to the eHealth Support Team at 1-844-630-0877.

AHS Facilities – A final signature must be obtained from Alberta Health. Please email completed forms to Alberta health privacy Team at AHPrivacy@gov.ab.ca.

**Purpose of the Alberta Netcare User Registration Form (URF)**

The URF is used by the appointed AA to manage user access to Alberta Netcare for affiliates of the custodian. Only authorized custodians and their affiliates can access Alberta Netcare.

**Completion of the Alberta Netcare URF**

The most current version of the URF, along with completion and submission instructions; is available through the Netcare Learning Centre: [http://www.albertanetcare.ca/1187.htm](http://www.albertanetcare.ca/1187.htm).

The eHealth Support Consultant can provide more assistance, if required. Contact information is available from the Alberta Netcare public website: [http://www.albertanetcare.ca/contact.htm](http://www.albertanetcare.ca/contact.htm).
Remote Access

Accessing Alberta Netcare from a site in the community is considered remote access. Remote access to Alberta Netcare is achieved through a web browser such as Internet Explorer (IE) or Firefox. Remote access can be requested when completing the URF and refers to the issuance of a token (also called a FOB).

Remote access tokens are used to securely access the Alberta Netcare Electronic Health Record (EHR) remotely from a community site. Tokens are a self-contained method for effective user identification. There are 2 options available:

- **Hard Token (FOB):** The hard token is a convenient, self-contained device that uses time, an algorithm, and a unique identifier for secure authentication to log in to the Alberta Netcare.
- **Soft Token:** The soft token is a software application available on a mobile device such as smartphones, tablets, and PCs. It will generate a code at regular intervals that can be used along with your access credentials to log in securely to the Alberta Netcare. Users must meet the soft token pre-requisites before selecting this option.

The Alberta Netcare AA is responsible for managing and administrating remote access to Alberta Netcare on behalf of their facility users and includes but is not limited to: requesting a token on behalf of the user if they require one; returning any hard tokens; providing guidance on token activations; and deactivating any tokens.

For more information on remote access and tokens please visit the Alberta Netcare Learning Centre: [http://www.albertanetcare.ca/LearningCentre/Access-Remote.htm](http://www.albertanetcare.ca/LearningCentre/Access-Remote.htm).

**IMPORTANT POINTS TO REMEMBER**

- The token whether hard or soft is issued to the user NOT the facility. The user is responsible for that token.
- The User CAN KEEP the hard token issued through one facility when working at multiple facilities.
- The AA MUST NOT keep any hard tokens at the facility. Remember tokens serve a role similar to a bank card, demonstrating that the individual trying to access the account is entitled to do so. Just as bank cards are not recycled and given to the next person to use, hard tokens should never be retained by the AA on behalf of the facility and given to a new staff member to use.
- Tokens are NOT transferable from one user to the next. Hard tokens MUST BE returned to the AHS Remote Access Team when remote access is no longer required by the user; or if the hard token has been distributed to the facility in error.
- User must meet soft token pre-requisites before requesting a soft token.
- For support regarding tokens and any remote access authentication issues please contact AHS remote access Team at 1-844-542-7876.

**PLEASE RETURN HARD TOKENS TO THE FOLLOWING ADDRESS:**

AHS Remote Access  
19th Floor CN Tower, Room 106  
10004-104th Avenue,  
Edmonton Alberta T5J 0K1
Alberta Netcare Access Administrator Guide

Alberta Netcare Permission Matrix and Role Assignments

The most current version of the Alberta Netcare Permission Matrix is located on the Alberta Netcare Learning Centre: [http://www.albertanetcare.ca/1187.htm](http://www.albertanetcare.ca/1187.htm)

Access to Alberta Netcare is based on the Alberta Netcare Permission Matrix which lists roles with corresponding access permissions. The AA will select a role based on the user’s duties to the custodian (“need to know”). Each role in the permission matrix comes with standard access, which is automatically assigned when the role is selected; and the optional access, which must be selected in order to be assigned.

The Netcare Permission Matrix identifies three major role types: Administration; Clinical; and Pharmacy. Within each major role type are related roles that have standard and optional access components. Certain roles may be restricted to certain professions because of what information the role allows the user access to (e.g. Event & Immunization History), or what the role allows the user to do (e.g. prescribe, dispense, create or update). Consequently it is important that the role assignment adhere to the HIA, Netcare rules, and be based on the job the user is doing for the custodian. The flow charts on the following pages called “Access Level Selection Flow Diagrams” are provided to assist AA’s with assigning an appropriate role to the user based on the Alberta Netcare Permission Matrix.

Linked Documents and Items

<table>
<thead>
<tr>
<th>Name</th>
<th>Owner</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netcare User Registration Form</td>
<td>Alberta Health</td>
<td>Alberta Learning Centre Custodian/Netcare AA Information</td>
</tr>
<tr>
<td>Netcare Access Administrator Form</td>
<td>Alberta Health</td>
<td>Alberta Learning Centre Custodian/Netcare AA Information</td>
</tr>
<tr>
<td>Netcare Permission Matrix</td>
<td>Alberta Health</td>
<td>Alberta Learning Centre Custodian/Netcare AA Information</td>
</tr>
<tr>
<td>PRIRP Form and Guide</td>
<td>Alberta Health</td>
<td>Alberta Learning Centre Custodian/Netcare AA Information</td>
</tr>
</tbody>
</table>

Alberta Netcare Access Administrator Guide Versions

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Revisions</th>
<th>Reviewers</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>April 2010</td>
<td>Revised the Access Administrator V1.5 Guide</td>
<td>Alberta Health Security</td>
</tr>
<tr>
<td>2.1</td>
<td>Feb 2012</td>
<td>Revised the Access Administrator V2.0 for access management through IAM tool.</td>
<td>Alberta Health Security</td>
</tr>
<tr>
<td>2.2</td>
<td>June 2012</td>
<td>Revised v2.1 due to IAM roll-back in May 2012</td>
<td>Alberta Health Security Deployment Team AHS IT Access Office</td>
</tr>
<tr>
<td>2.3</td>
<td>July 2012</td>
<td>Revised Alberta Health logo and User Group Workflow – Pharmacy Diagram.</td>
<td>Alberta Health Security Deployment Team</td>
</tr>
<tr>
<td>3.0</td>
<td>March 2013</td>
<td>Alberta Netcare Form changes, matrix and update to Netcare AA Guide.</td>
<td>Alberta Health Security Deployment Team AHS IT Access EHR Team Provincial Service Desk</td>
</tr>
<tr>
<td>Version</td>
<td>Date</td>
<td>Description</td>
<td>Team</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>3.0</td>
<td>May 2013</td>
<td>Reviewer name update – ICAU and Privacy &amp; Security changed to Alberta Health Security. Update to remote access section.</td>
<td>Alberta Health Security</td>
</tr>
<tr>
<td>3.1</td>
<td>May 2015</td>
<td>Revised links, contact information. Updated section information: remote access, breach, flow diagrams.</td>
<td>AH Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>AH Privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EHR Deployment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>AHS IT Access</td>
</tr>
<tr>
<td>3.2</td>
<td>June 2016</td>
<td>(minor) Revise branch name due to re-org. Revise unit name. Update the contact number for Remote Access.</td>
<td>AH Privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EHR Deployment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>eHSS Team</td>
</tr>
</tbody>
</table>
Access Level Selection Flow Diagrams

1. Clinical Access:

   Begin
   
   Patient Information Type
   
   Demographic Only
   
   Most Appropriate Job Function
   
   General Clinical Support – (RN, LPN, Therapists, Unit Clerk, etc.)
   
   General Clinical Support (Lab Technologist, Lab Staff)
   
   Licensed Physician, Nurse Practitioner
   
   Physician in Training (Resident/Fellow/Students/Physician Assistant/Nurse Practitioner Student)
   
   General Clinical Support - No Lab
   
   General Clinical - Name or ID Search, PIN + PD only (Admin Support, Clerks, Health Records)
   
   Search Type
   
   ID Search Only
   
   Clinical 5
   
   Clinical 2
   
   Search by Patient ID
   
   Yes
   
   Clinical 7
   
   No
   
   Transcribed Reports
   
   Yes
   
   Clinical 8
   
   No
   
   Clinical 10
   
   Yes
   
   Clinical 11
   
   Lloyd Hospital
   
   Yes
   
   Clinical 9
   
   No
   
   Clinical 4
   
   Yes
   
   Clinical 1
   
   No
   
   Clinical 2
2. Administration Access:

NOTE: no PIN access on Admin access levels
3. Pharmacy Access:

- Yes
- No

Yes

Pharmacist/Intern/Pharmacy Student?

Pharmacy 2

No

Pharmacy Technician?

Pharmacy 4

Pharmacy 5