Fact Sheet
Access Certification
AHS IAM Identity Record (AHS Network Access)

Contents

What is changing?

Access Certification for AHS IAM Identity Records (AHS Network Access) is now mandatory, not optional, for AHS Non-Employees and certain Physicians. Authorized Approvers for these people must deliberately extend their access before their access' Sunset / Expiry Date. If they don't, it will be disabled.

Back to top

Who will be impacted by this change?

Access Certification will change from optional to mandatory for AHS Non-employees and certain Physicians.

How Access Certification will impact AHS "Non-Employees"

AHS Non-Employees are not on-boarded or paid through the AHS Human Resources e-People. These End-users and their Authorized Approvers are sent email notifications 30, 15 and 2 days in advance of their Identity Sunset / Expiry Date. Emails are personalized, provide the Sunset / Expiry Date, and instructions on what to do.

How Access Certification will or will not impact Physicians

Employee Physicians - Members of the AHS Medical Staff

- These physicians are managed by the AHS Medical Affairs feed.
- These physicians are hired and paid through AHS e-People.
- They are classified as "AHS employees" and sometimes also as "AHS non-employee" end-users.
- These physicians are excluded from Access Certification because their access is automatically managed between e-People and IAM.

Non-Employee Physicians – Members of AHS Medical Staff

- These physicians are members of the AHS Medical Staff and may be privileged at AHS, Covenant Health or Affiliate facilities.
- These physicians are managed by the Medical Affairs feed.
- These physicians are not managed by AHS e-People.
- They are given access to the AHS Network and AHS IT systems. Their AHS network access is automated through the connection between the Medical Affairs feed and IAM.
- They are not included in Access Certification.

Non-Employee Physicians – not members of AHS Medical Staff

- These physicians are not members of the AHS Medical Staff and are not privileged at AHS facilities, but many are given access to the AHS network and AHS IT systems.
- These physicians are not managed by the Medical Affairs feed and are not managed by AHS e-People.
- AHS network and IT system access is managed for these physicians by their clinic's Access Administrator (aka Authorized Approver). Some Access Administrators have access to IAM while others use manual processes. If a manual process is used, IT Access Services enter the information into IAM.
- These physicians are included in both Alberta Netcare Portal and AHS Identity Access Certification. ANP Access Certification takes precedence. If ANP access is extended, then the AHS Identity is automatically extended as well.
- They and their Access Administrators are sent email notification from IAM at 30, 15 and 2-days before the access' Sunset / Expiry Date.
- Please note that emails stop being sent as soon as action is taken by the Authorized Approver.
- If access is extended, Access Certification starts again 30 days before the next Sunset / Expiry Date.

Back to top

When does this change start?

This change to Access Certification for AHS IAM Identity Records (AHS Network Access) is effective on July 7, 2022.

Advance notice was circulated in a variety of communications and posted on the IAM Login Page since May of 2022.

Why are we doing this?

These changes are directed by the AHS Information Cyber Security Council (ICSC), Provincial Technology Services, per Briefing Note November 2021.

Unused and incorrect access presents an unacceptable security risk to Alberta Health Services, its systems, data, and end-users. Automating these security practices upholds the AHS IT security framework in the face of growing cyber security threats world-wide.

Authorized Approvers who set up AHS Network access for AHS Non-Employees are reminded to keep access current and correct at all times.

Will I be notified in advance?

Yes. All end-users and their Authorized Approver on record (usually the person's manager), or their clinic's Access Administrator, will be sent automated email notifications from "Identity Management", the Identity & Access Management (IAM) system.

Email notifications will be sent at 30, 15 and 2 days prior to the Identity Record's Sunset / Expiry date. All notifications are personalized by name, provide the Sunset / Expiry date, and include instructions on what to do.

What is AHS Network Access Certification?

Access Certification is a vital security practice that does four things.

1. It ensures that the correct Authorized Approver is associated with every person's AHS IAM Identity Record (AHS Network Access).

2. It verifies that access is still required.

3. It deliberately extends required access to no more than one-year in the future when it must be certified again.

4. It deliberately removes access that is not required to prevent security risks.

How is Access Certification done?

Instructions are provided in personalized email notifications sent to both the end-user and their Authorized Approver on record. They have a shared responsibility to ensure that access to the AHS Network is valid and correct.

The Authorized Approver is provided with a direct link to their Access Certification page in the Identity & Access Management (IAM) system. That page lists all the people whose access they are responsible for.

For each end-user, the Authorized Approver must do as follows.

1. **Ensure they are still the correct Authorized Approver for each person.** If they are not, they must perform the "Not Mine" action. This initiates a process of identifying a new Authorized Approver for that end-user.

2. **Verify that the access is still required.**

3. **If the end-user still needs AHS Network Access, the Authorized Approver must "Extend" the access**. If this action is not done on time, the end-user's AHS IAM Identity Record (AHS Network Access) will be disabled on the Sunset / Expiry Date.

   This is the key change – this type of access used to be automatically extended. That is not so anymore. The access must be deliberately extended by the Authorized Approver.

4. **If access is no longer needed, the Authorized Approver must "Remove" the access.**

Reminders for Authorized Approvers

If you are an Authorized Approver, you are obligated to actively monitor the AHS network access used by your direct reports. When a direct report "AHS non-employee" leaves AHS, it is vital that you remove their network access using IAM and the NAR Remove Access process.

As the Authorized Approver on record, you are responsible for:
- Authorizing appropriate access to the AHS network and its systems
- Ensuring that appropriate action is taken in the event of a security beach by the end-user
- Ensuring that action is redirected if the person no longer reports to you
- Ensuring that access is removed when it is no longer required.

How can I get my AHS Network Access back if it is disabled?

Physicians should contact their clinic's Access Administrator (Authorized Approver) or their AHS Medical Affairs office.

AHS non-employees, talk to your Authorized Approver. If you both agree that you still need access to the AHS Network, your Authorized Approver should log into the AHS Identity & Access Management (AHS IAM) system, and submit a "Network Access Request-Enable" request for you.

The Network Access Request (NAR) User Guide is available on the AHS IAM Support Page under Learning.

Back to top

What if I don't need AHS Network access anymore?

You can let your access expire if you no longer need it. Only maintain Network access if it is relevant to your job role now. Discuss this with your Manager / Authorized Approver. Remember the Health Information Act of Alberta states you should access the least amount of information needed to perform your job role.

Back to top

◆ end ◆