NDHIN
North Dakota Health Information Network
Quality Healthcare for All North Dakotans, Anywhere, Anytime.

Requesting a Direct Secure Messaging Account

The Orion Health Direct Secure Messaging system (DSM) allows users at your Healthcare Organization (HCO) to send and receive healthcare information using the Direct network. This document provides instruction on how to request access to the Direct network.

Membership of the Direct network requires identity verification to ensure that only authorized HCOs are able to use the network. In order to meet these identity verification requirements, an organization representative is required to provide an identity declaration and have it notarized.

The notarized Declaration of Identity form requires information for the HCO that the Direct digital certificate will be issued for and an authorized representative of that HCO. It authorizes Orion Health to issue Direct digital certificates on behalf of the HCO.

The Direct Network is accessed through DSM Web.

	DSM Web
Description	DSM Web is a web-based secure mail solution that provides an easy to use method for sending and receiving Direct messages.
Selection Criteria	DSM Web should be used by organizations looking for a user interface for sending and receiving Direct messages.

You will need to fill out the DSM Web Account Request form.

The Account Request form contains requested details about the HCO's Direct account. This includes organization details such as name and the email domain requested. For DSM Web it includes a list of people who will be given administrator logins to the DSM Web Account Management Portal in order to approve users of individual Direct email addresses.

Steps to complete signup

1. Complete Request HCO Account Form

Complete the DSM Web Account Request.

A representative with authority to sign documents on behalf of the organization must complete the Account Request form.

2. Gather Required Identification

The representative supplies suitable identification for verification.

a A government-issued photo ID that lists the representative's name and address.
   - Examples of acceptable photo ID documents include a passport, driver's license, military ID, permanent resident card, or similar document.

b If the ID is not a federal government ID, a secondary ID is required.
   - The second ID does not have to be a government-issued ID.
   - Examples of acceptable secondary ID documents include a social security card, birth certificate, school ID, or voter's registration card.

c If the address on the ID is not correct (as filled out in the Declaration of Identity form), a document showing the correct address is required.
   - Examples of acceptable proof of address include a utility bill (telephone, gas, electric, water or Internet), bank statement, rental agreement or a government-issued document.
   - You may block out any sensitive information, as long as it shows the name and address.

3. Complete Declaration of Identity Form

The Declaration of Identity form must be printed out and completed on paper in accordance with the following instructions to issue a Direct certificate for your organization. Direct certificates are required to securely transmit health care information using DSM. Any failure to follow these instructions may result in a delay in issuing the certificate.

By signing the Identity Verification, you also agree to the attached authorization for certificates. This authorization gives Orion Health permission to request and use certificates in your name. Orion Health will only use the certificates to transfer health care information to and from your organization in accordance with the Direct Protocol.

The following section provides additional information for the completion of the Declaration of Identity.

a. Service Provider Section

Do not alter this section. It has been pre-filled with the correct information.

b. Organization Section

Enter your organization name and contact details.

This will be checked against a public registry to verify that the organization is a real health care organization. Please ensure that the details are correct, otherwise there may be a delay in issuing the Direct certificate.

c. Applicant Section

This section should contain the details of the HCO representative who is filling out the application. The details entered here must match those in the identification documents provided. If the address does not match the one on the representative's primary identification, a proof of address document must be provided as well.

d. Signature

Do not sign the document yet. Your signature must be witnessed by a notary.

4. Notarize Declaration of Identity

Take the completed paper copy of the Declaration of Identity form and your identification documents to a notary for attestation. The notary must see you sign the Declaration of Identity form. The notary must then fill out their part of the Declaration of Identity form and sign.

5. Create Digital Copy of Declaration of Identity

Create a digital copy of the signed, notarized Declaration of Identity form. The digital copies of the signed documents must either be PDFs or image files. We recommend using a scanner or digital camera to make the digital copy. Please ensure the digital copies are clearly legible to assist with the identity verification process.

6. Submit Documents

Send the following documents as attachments in an email to your HIE:

- the digital copy of the notarized Declaration of Identity form
- the completed Account Request Account form

Please clearly identify the email message as "Completed DSM Account Request Documentation" in the email subject.

What's Next

1. Your HIE will verify the information, and approve if appropriate
2. Your HCO will be issued a Direct certificate upon verification of the identity material
3. You will be sent a welcome pack by email. The welcome pack includes:
    - Instructions on how to access the DSM system
    - All the necessary forms.
        - Add Organization Administrator form
        - Remove Organization Administrator form
        - Disable HCO Account form