# DataMotion Direct Provisioning Portal Administration Guide

May 11, 2018

Part # 050041–02

*DataMotion Direct Provisioning Portal Administration Guide v2*

Publication Date: May 11, 2018

Printed in the United States of America.

**DataMotion, Inc. Confidential and Proprietary Information.**

Published By:

DataMotion, Inc.
200 Park Ave,
Florham Park, NJ 07932
USA

1 800-672-7233

http://www.datamotion.com/

# TABLE OF CONTENTS

ABOUT THIS PUBLICATION 10

INTENDED AUDIENCE ........ 10
TERMINOLOGY ........ 10
Organizational Roles ........ 10
Hierarchical Terminology ........ 11
Other Terminology ........ 11
Synonyms ........ 12
HOW TO USE THIS PUBLICATION ........ 12
RELATED INFORMATION ........ 13
DataMotion Documentation ........ 13

1 INTRODUCTION 14

ABOUT THE DATAMOTION DIRECT PROVISIONING PORTAL ........ 14
VALIDATION AND ENABLING A TRUSTED SERVICE ........ 14
OUTLINE OF THE ONBOARDING PROCESS ........ 15
Readying Proper Identity Information ........ 15
User Required Information ........ 15
Organization Required Information ........ 15
Company Provisioning ........ 16
Request Certificate ........ 16
Provision Users ........ 16

## 2 Getting Started 17

**ESTABLISH YOUR ACCOUNT .......... 17**
- Creating Your Login Credentials .......... 17
- Log Into Your Account .......... 19
- Changing Your Password .......... 19
- Reset Your Password .......... 21

**NAVIGATION .......... 23**
- Home .......... 23
- Tenants Tab .......... 24
- Users Tab .......... 24
- Domains Tab .......... 25
- Certificates Tab .......... 26
- Reports .......... 29
- Support .......... 30

## 3 Organizational Provisioning 31

**PROVISION A TENANT ORGANIZATION .......... 31**
- Prerequisites .......... 31
  - Government Issued ID Requirements .......... 31
  - NOTE Regarding Photo ID Submission .......... 32
  - Company Information .......... 33
- Create Organization .......... 33
  - Step 1: Organization Information (Create Organization) .......... 35
  - Step 2: Domain Information (Create Organization) .......... 37
  - Step 3: Authorized User (Create Organization) .......... 38
  - Step 4: Verify Your Organization (Create Organization) .......... 39
- Register Organization .......... 40
  - Step 1: Organization Information (Register Organization) .......... 41

Step 2: Domain Information (Register Organization) .......... 44
Step 3: Authorized User (Register Organization) .......... 45
Step 4: How would you like your alerts to be communicated? .......... 46
Step 5: Verify Your Organization (Register Organization) .......... 46

4 TRUSTED AGENT ACTIONS 48

CERTIFICATE REQUESTS .......... 48
Organizational Certificate Request .......... 48
Address Certificate Request .......... 50
Revoking a Certificate .......... 51
Renew a Certificate .......... 52
Rekey a Certificate .......... 53
EDITING USERS .......... 54
CREATING A NEW TRUSTED AGENT .......... 57

5 ADMINISTRATIVE ACTIONS 61

USER PROVISIONING .......... 61
Adding a Single Direct User .......... 61
Adding a Direct User covered by an Address Certificate .......... 62
Adding a Direct User covered by an Organization Certificate .......... 65
Adding an Administrative User .......... 69
Provisioning Multiple Direct Users via Bulk Import .......... 71
Bulk Import for users covered under an organization certificate .......... 72
Bulk Import for users covered under address certificates .......... 75
Bulk Import for users covered by Patient certificates .......... 77
RE-SENDING NOTIFICATIONS (RETRY PROVISIONING) .......... 80

**DELETING USERS ..... 80**
Deleting a Trusted Agent ..... 81
Deleting Direct Users ..... 81
Deleting a Non-TA Administrator ..... 81
**ADDING AND VALIDATING A DOMAIN ..... 82**
**EDITING AN HCO ..... 83**
**DELETING AN ORGANIZATION ..... 85**
**ADDING AND REGISTERING CHILD ORGANIZATIONS ..... 86**
Adding a Child Organization ..... 86
**REPORTS AND LOGGING ..... 86**
Message Tracking Report ..... 88
User Logon Report ..... 88
User Reports ..... 90
Total View Report ..... 91
ONC Reports ..... 93
IM1 ..... 94
IM2 ..... 94
IM3 ..... 95
IM4 ..... 96
IM5 ..... 96
IM6 ..... 97
IM13 ..... 98
IM14 ..... 98
IM15 ..... 99
Onboarding Reports ..... 100
Organizations Onboarded ..... 100
Users Onboarded ..... 101
Certificate Report ..... 102
Audit Logs and Notifications ..... 103

## TABLE OF FIGURES

Figure 1 – Creating a new account ..... 17
Figure 2 – Setting your account password ..... 18
Figure 3 – Logging into your Provisioning Account ..... 19
Figure 4 – Changing your password ..... 20
Figure 5 – Reset Password Page ..... 22
Figure 6 – Home screen controls ..... 23
Figure 7 – Tenants Tab ..... 24
Figure 8 – Users Tab ..... 25
Figure 9 – Domains Tab ..... 26
Figure 10 – Certificate screen controls ..... 27
Figure 11 – Reports screen controls ..... 29
Figure 12 – Support Requests and Documentation ..... 30
Figure 13 – Adding a tenant company ..... 33
Figure 14 – Create a Healthcare Organization Step 1 (Organization Information) ..... 35
Figure 15 – Create a Healthcare Organization Step 2 Domain Information ..... 37
Figure 16 – Create a Healthcare Organization Step 3 Authorized User ..... 38
Figure 17 – Create a Healthcare Organization Step 4 Verify Your Organization ..... 39
Figure 18 – Register a Healthcare Organization Process ..... 41
Figure 19 – Register a Healthcare Organization Step 1 Organization Information ..... 42
Figure 20 – Register a Healthcare Organization Step 2 Domain Information ..... 44
Figure 21 – Register a Healthcare Organization Step 3 Authorized User ..... 45
Figure 22 – Register a Healthcare Organization Step 4 Communication Alerts ..... 46
Figure 23 – Register a Healthcare Organization Step 5 Verify Your Organization ..... 47
Figure 24 – Request an Organization Certificate ..... 49
Figure 25 – Request an Address Certificate ..... 50
Figure 26 – Revoke Certificate ..... 52
Figure 27 – Edit User ..... 56
Figure 28 – Create a new TA User for the organization Part A ..... 58
Figure 29 – Creating a new TA User for the organization Part B ..... 59
Figure 30 – Adding an Address Certificate Subscriber (ACS) Direct User Part A ..... 63
Figure 31 – Adding an Address Certificate Subscriber (ACS) Direct User Part B ..... 65
Figure 32 – Adding a Direct User covered under an Organization Certificate Part A ..... 67
Figure 33 – Adding a Direct User covered under an Organization Certificate Part B ..... 68

Figure 34 – Adding an Admin User Part A .... 70
Figure 35 – Adding an Admin User Part B .... 70
Figure 36 – Submitting a CSV via Bulk Import .... 71
Figure 37 – Validating an organization's domain .... 82
Figure 38 – Edit a Healthcare Organization page .... 85
Figure 39 – Deleting an organization .... 86
Figure 40 – Reports page .... 87
Figure 41 – Message Tracking Report Results .... 88
Figure 42 – User Logon Report Results .... 90
Figure 43 – User Reports Type Result .... 91

# REVISION HISTORY

This section summarizes significant changes, corrections, and additions to the document. The history appears in chronological order with the most recent changes listed first.

## Version 2

This version has been updated to include new features allowing Admins and Trusted Agents to perform more administrative tasks. This includes an update to bulk import allowing users to be provisioned with additional information, the ability to re-send notifications, and the ability to bulk delete users.

- *Chapter 4) Trusted Agent Actions:*
  - *Renew a Certificate* (on page 52)
    Added this section which describes how a Trusted Agent can renew a certificate.
  - *Rekey a Certificate* (on page 53)
    Added this section which describes how a Trusted Agent can rekey a certificate.
- *Chapter 5) Administrative Actions:*
  - *Bulk Import for users covered under an organization certificate* (on page 72)
    Updated this section to include text about how an Admin or Trusted Agent can have user information match the organization they are provisioned under or use the information provided in the spreadsheet.
  - *Bulk Import for users covered under address certificates* (on page 75)
    Updated this section to include text about how an Admin or Trusted Agent can have user information match the organization they are provisioned under or use the information provided in the spreadsheet.
  - *Re-Sending Notifications (Retry Provisioning)* (on page 80)
    Added this section which describes how an Admin or Trusted Agent can re-send any provisioning notifications to users.
  - *Deleting Users* (on page 80)
    Updated this section to include text about how an Admin or Trusted Agent can delete multiple users due to the new checkbox selection method.

## Version 1

Initial version of this document, for DPP.

# About This Publication

## INTENDED AUDIENCE

The purpose of this information is to describe the onboarding and provisioning process performed by using the DataMotion Direct Provisioning Portal, or DPP. This publication is primarily intended for administrators of healthcare organizations (HCOs) that have enabled the use of DataMotion Direct Secure Messaging. They are not expected to be security experts. It is helpful if the reader is familiar with Direct Secure Messaging, as well as with navigating the Internet with a web browser such as Internet Explorer, Chrome, Firefox, Safari, and Opera.

The user interface has been designed for simplicity and ease so that administrators can onboard and provision Direct Messaging accounts quickly and easily.

## TERMINOLOGY

### ORGANIZATIONAL ROLES

- Health Information Service Provider (HISP): An entity that relays medical data using Direct protocols. As a HISP, DataMotion assigns and maintains the Direct email addresses for EHRs, HIEs, and individual providers and relays their medical data securely using Direct protocols.
- Healthcare Organization (HCO): Any organization that serves, services, or supports the delivery of healthcare, including healthcare providers, doctors, laboratories, hospitals, pharmacies, health insurance providers, business associates, HIEs, EHRs, etc.
- Health Information Exchange (HIE): A regional network that enables providers to establish and maintain communications over Direct.
- Electronic Health Record (EHR) Vendor: An organization that manages Electronic Health Records and communicates over Direct. EHRs are certified by a standards body responsible for the Direct program certification, such as the Certification Commission for Health Information Technology (CCHIT).
- Registration Authority (RA): Responsible for Identity Verification at the organizational and individual levels. The RA services can be provided by a separate organization from the CA, or both CA and RA services can be provided by the same organization. DataMotion coordinates RA services as part of DataMotion Direct.

- Certification Authority (CA): Responsible for Digital Certificate issuance, management, and revocation. DataMotion coordinates CA services as part of DataMotion Direct.
- Provider (End User): An office with at least one doctor. The provider communicates through a Direct email address with other Direct users.
- Trusted Agent (TA): An identity-vetted individual with authorization to perform the following tasks related to the registration process and certification process: verify credentials for future TA applicants (sign future Declaration of Identity documents), be named on a certificate application (as the organization representative), and request certificates on behalf of other users/organizations.
- Address Certificate Subscriber (ACS): An individual to be named on an Address Certificate as the recipient. This individual must be identity vetted (through the same process as a TA), and upon validation, may obtain a certificate bound to a desired Direct address.
- Authorized User (or Administrator): The user that is acting in this row shall have the capabilities to do most if not all tasks related to company and user provisioning. This user is also capable of creating child organizations and fully registering additional authorized users for them as long as they are below them in the hierarchical tree.
- Information Systems Security Officer (ISSO): A person at the HISP who is responsible for managing the registration process, certificate requests, and private keys for Direct. This includes ensuring adequate protection of cryptographic keys held on behalf of customers, and also for tracking and recording exactly who has access to the keys at any given point.
- Certificate Revocation List (CRL): A list that is generated whenever a certificate is removed from the HISP.

## HIERARCHICAL TERMINOLOGY

The DPP provisions users in a multi-tenant architecture. This means that each tenant company is provisioned by its host company. For example, a large scale EHR may have a multitude of healthcare providers using its systems that require Direct Messaging. This EHR would provision all of these providers as Tenants on the DPP under itself. The EHR would then have visibility into all of these Tenant companies and children of those tenants.

- Host Company: Also known as a Parent Company, a Host Company is the company that exists one level above your company in the hierarchy. For example, DataMotion is the Host/Parent Company of a reseller partner.
- Tenant Company: Also known as a Child Company, a Tenant Company is the company that exists one level below your company in the hierarchy. For example, a reseller partner is a Tenant/Child Company of DataMotion.

## OTHER TERMINOLOGY

- Declaration of Identity (DoID): An electronic/paper form that is used by DataMotion to collect information of an individual that requires identity validation. The Applicant must present a paper copy of the DoID, along with at least one valid government-issued photo ID, to either a Notary public, or an already validated TA. Appended to the DoID is a Certificate Authorization.

- Organizational Certificate (Org Cert): A digital certificate that is bound to a Direct-specific domain (i.e.: direct.MyTownHospital.com). The organization representative is a validated TA that is named on the certificate application. Because an org cert is bound to a domain, any Direct addresses created with that same domain will be covered by the org cert.
- Address Certificate (Address Cert): A digital certificate that is bound to a specific Direct messaging address (i.e.: douglasjones@direct.healthcare.org). Before creating the Direct messaging address, the individual must undergo the same identity validation process as a Trusted Agent (see Address Certificate Subscriber above)

### SYNONYMS

Sometimes the DataMotion Direct Provisioning Portal features and components have acquired synonyms or short-hand names in this documentation that are useful to know.

The following table provides synonyms that you may encounter. The synonyms may refer to a component or an identifiable part of a component.

**Table 1 – Synonyms**

| Component | Sometimes Referred to as: |
|---|---|
| DataMotion Direct Provisioning Portal | Direct Provisioning Portal<br>Provisioning Portal<br>DPP |
| DataMotion Direct Messaging Portal | Direct Messaging Portal or DMP |
| Declaration of Identity | DoID |
| Identity Validation | ID Validation<br>ID Vetting |
| Healthcare Provider Directory | HPD |
| Organization Certificate | Organizational Cert<br>Org Cert |
| Address Certificate | Address Cert<br>Individual Certificate<br>Individual Cert |

## HOW TO USE THIS PUBLICATION

The *DataMotion Direct Provisioning Portal Administration Guide* provides detailed instructions for using the product.

The content is organized as follows:

*About This Publication*.

Provides a description of the content of this publication and how to use the publication.

*Chapter 1) Introduction*

Provides an introduction to the DPP as well as an outline of the onboarding process.

*Chapter 2) Getting Started*

Describes how to activate and access your DPP account, as well as a brief description of the layout of the portal.

*Chapter 3) Organizational Provisioning*

Describes the registration process for adding an organization.

*Chapter 4) Trusted Agent Actions*

Describes the common actions that can be performed by a Trusted Agent on the DPP, and provides instructions to perform those tasks.

*Chapter 5) Administrative Actions*

Describes the common actions that can be performed by an Administrator on the DPP, and provides instructions to perform those tasks.

## RELATED INFORMATION

### DATAMOTION DOCUMENTATION

- *DataMotion Direct Software Development Kit Technical Reference Manual* (part # 050001)
  Documents the Application Programming Interfaces (APIs) for messaging and administration, system development, maintenance, and administration tools for developers.
- *DataMotion Direct User Guide* (part # 050003)
  Provides instructions for using the products.
- *DataMotion Direct Administration Guide* (part # 050005)
  Documents the system installation, maintenance, and administration tools for administrators and integrators. This is the original guide that pre-dates the release of the DPP.
- *DataMotion Direct Messaging Portal Administration Guide* (part # 050040)
  Documents the features still available to Admin users on the messaging portal. This document is a re-created version of the original guide listed above due to the release of DPP and the subsequent removal of numerous messaging portal admin features.
- *DataMotion Direct Provisioning Reference Manual* (part # 050042)
  Documents the provisioning API for the DPP including the required fields for requests, responses, and possible errors.

Additional documentation is available on many other topics. Please contact DataMotion Customer Service for more information.

# 1
# Introduction

## ABOUT THE DATAMOTION DIRECT PROVISIONING PORTAL

The DataMotion Direct Provisioning Portal, or DPP, is a self-service, web-based portal that simplifies, automates, and expedites the process of implementing Direct Secure Messaging. The DPP combines user registration, certification, and management into a single web portal that offers the ability to use Direct Secure Messaging to healthcare organizations of any size. The intuitive, user friendly interface eliminates the complexity involved in validating identities, obtaining digital certificates, and onboarding, provisioning and managing Direct accounts.

By simplifying and automating the steps required to implement Direct Secure Messaging, the DPP drastically reduces the barrier to entry to Direct for healthcare organizations of all sizes. The DPP handles all aspects of onboarding, from identity validation to onboarding and provisioning users. For on-boarded users, the DPP provides a centralized reporting interface for all compliance needs, including the ONC reports required to meet the MU2 attestation criteria, and the collection of healthcare provider information for the DataMotion Healthcare Provider Directory (HPD).

The DPP will be utilized by a broad spectrum of the healthcare field. This includes healthcare providers, care team members, patients, laboratories, hospitals, clinical systems, pharmacies, business associates, and health insurance providers.

## VALIDATION AND ENABLING A TRUSTED SERVICE

For the majority of actions taken on the DPP to be approved, a manual accept/deny will have to be performed via a DataMotion Officer. This manual approval will be performed as soon as possible, but the approval time may vary.

DataMotion provides a way to bypass manual validation via a Trusted Service for the DataMotion Direct Provisioning API. Once a Trusted Service is designated within a company, it will be possible to use the DataMotion Direct Provisioning API to send requests that will automatically validate.

**WARNING! With Trusted Service enabled, the protections that are normally provided by a DataMotion Officer validating certificate-based requests will no longer be in**

**place. For example, if you have Trusted Service enabled and revoke an Organization certificate using the API, it will immediately terminate all account capabilities that are based on this certificate being valid. This includes account functions and Direct messaging send/receive capabilities for all users in the organization who are covered under the certificate, such as all TAs and admins. If instead you have Trusted Service disabled (which is by default) and revoke an Organization certificate, DataMotion would review the request.**

**NOTE: Trusted Service does not apply to the operations through the portal. Any Attempts to login to the DPP with the Trusted Service credentials will fail as a result of this.**

The Trusted Service feature is not included by default within a company upon creation and can only be applied by DataMotion itself. A request can be put in to designate a company as a Trusted Service by contacting DataMotion Support (directsupport@datamotion.com). You will be required to provide a completed Declaration of Identity Document to the support staff in order to have the request approved.

## OUTLINE OF THE ONBOARDING PROCESS

Onboarding companies and users can be a convoluted process without the required prerequisite documents and information that would be required, set up and ready to go beforehand. Following the sub-sections in order will help you to understand the process before attempting it live. The sections themselves are equivalent to steps and should be performed in sequential order, with latter steps assuming that all former steps have been completed.

### READYING PROPER IDENTITY INFORMATION

A crucial step to performing organization and user provisioning involves the submission of valid identification materials to the DataMotion CA/RA in order to be successfully provisioned to the portal.

#### User Required Information

The identity information that will be required must include either a federally issued ID or a photo-ID, and be REAL ID compliant (see the Department of Homeland Security's information regarding REAL ID at the following site http://www.dhs.gov/real-id-public-faqs). A second ID will be required if these needs are not met.

#### Organization Required Information

General information regarding the HCO's name and address will be needed to complete the onboarding process and should be readily available. In addition to basic information, an Organization NPI, EIN, or Business License will be required for validation purposes so have at least one of these items available.

## COMPANY PROVISIONING

After readying the appropriate information, an organization must be provisioned in order for Direct messaging to be possible. Proceed to the ***Register Organization*** section if a company and TA has already been created (typical for first time users or subsidiaries of larger HCO's). For those who exist on the DPP already and need another company, head to the ***Create Organization*** section.

## REQUEST CERTIFICATE

Assuming a Trusted Agent and a domain were created a certificate, request must be performed. Depending on the certificate type the domain will accept see either the ***Organizational Certificate Request*** or the ***Address Certificate Request*** sections.

## PROVISION USERS

When the certificate is validated it will be possible to add users to the company. Proceed to the ***Adding a Single Direct User*** or ***Provisioning Multiple Direct Users via Bulk Import*** sections in order to add users who are enabled for Direct messaging.

# 2
# Getting Started

## ESTABLISH YOUR ACCOUNT

### CREATING YOUR LOGIN CREDENTIALS

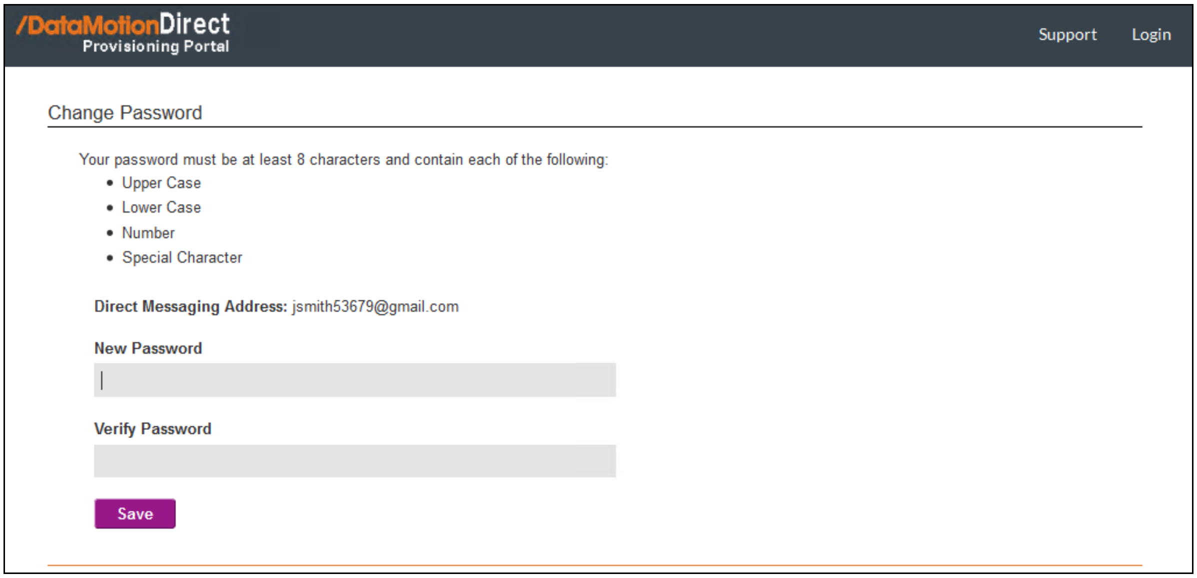
The first step to using the DataMotion Direct is to establish your account and password. When your account is created (by your parent organization), an email notification will be sent to the email address associated with your DataMotion Direct account. This email contains a link to create your DataMotion Direct account password.

**NOTE: Depending on your email settings or choice of client it is possible that the notification email will end up in the Spam folder. Do not delete it.**

**Figure 1 – Creating a new account**

The link in the email notification will open your web browser and take you to the following page:

**Figure 2 – Setting your account password**




In the first text box, you must enter a password that meets the criteria in the image above. Upon verifying the password in the second text box, click Save to log in.

## LOG INTO YOUR ACCOUNT

**Figure 3 – Logging into your Provisioning Account**


To access your DataMotion Direct Provisioning Portal account:

1. Use your web browser to navigate to the DPP site: https://admin.dmhisp.com
2. Enter your notification email address and the password in the login window.
3. Click Sign in to login.

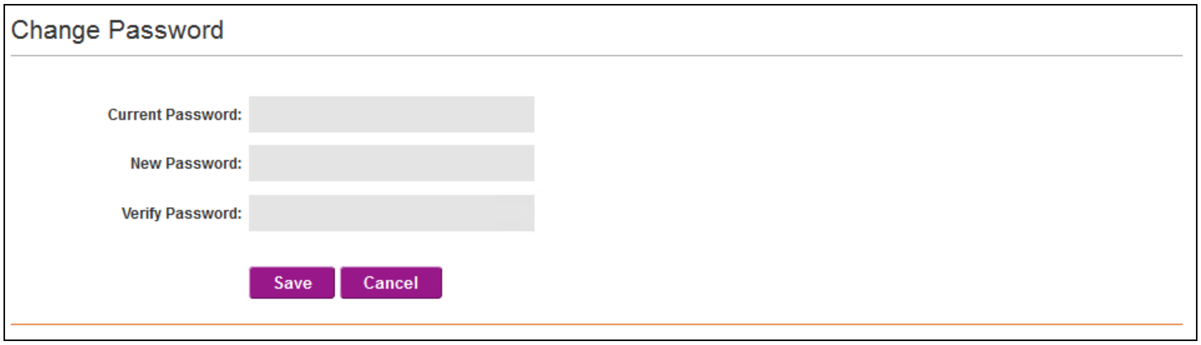
## CHANGING YOUR PASSWORD

In the event that you would like to change your password it is possible to do by performing the following steps.

1. Click on your username (this can be performed from anywhere on the portal).

2. Select **Change Password** from the drop-down.
3. Enter your **Current Password**, the **New Password**, and re-enter your new password in the **Verify Password** field.
4. Click the **Save** button to finish.

**Figure 4 – Changing your password**

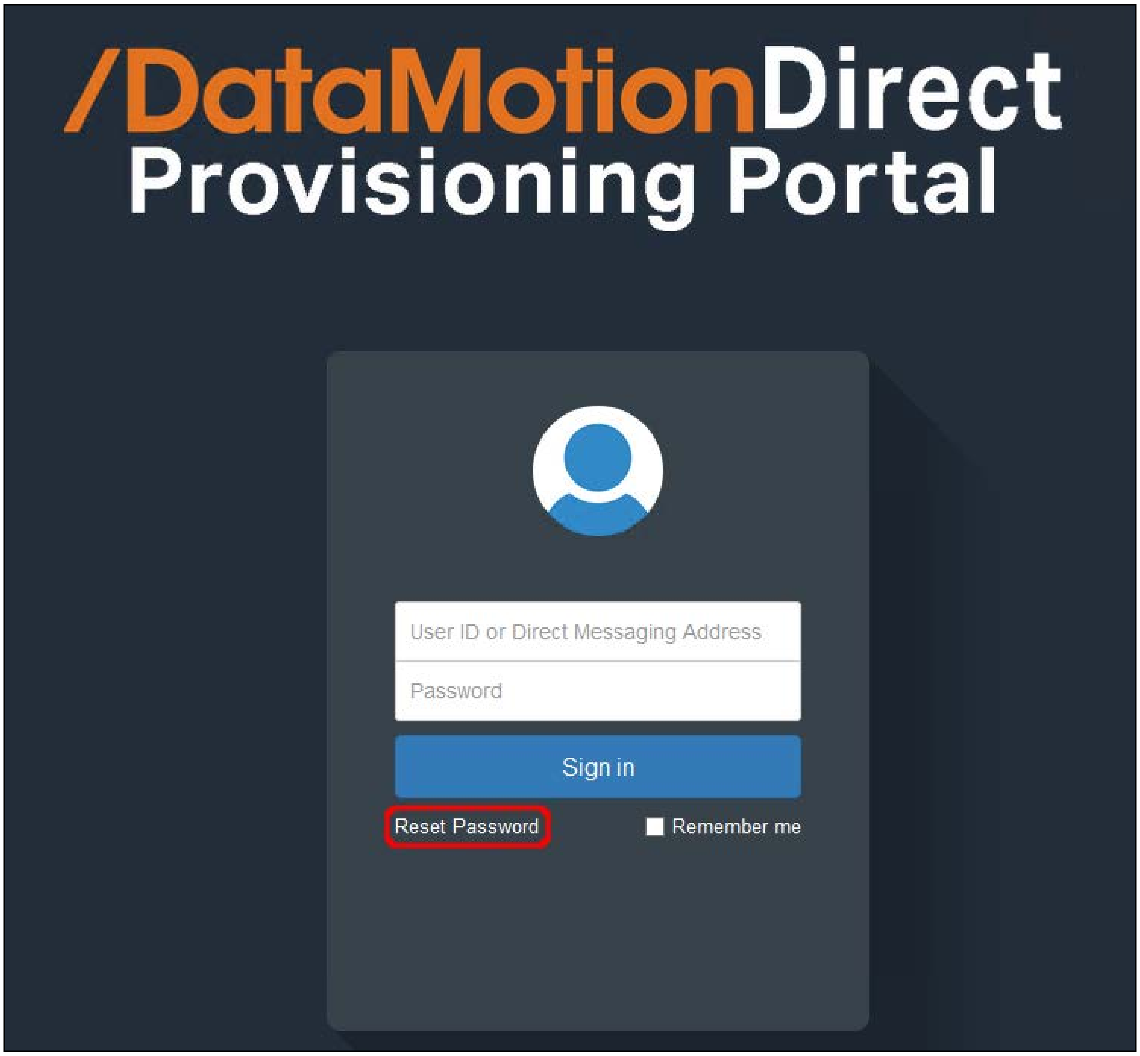


## RESET YOUR PASSWORD

If you ever forget your password it is possible to request a password reset. The response will be an email notification sent to the email address that you used to sign up to the DataMotion Direct Provisioning Portal.

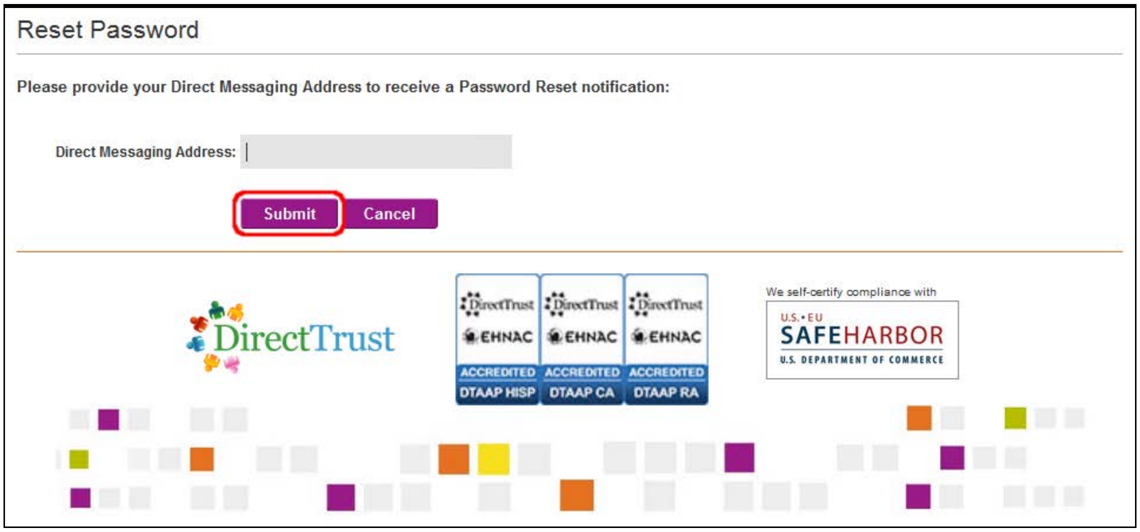
The following steps describe how to initiate a password reset.

1. On the Sign in page, click the Reset Password link.




2. Enter the email address that received the DataMotion Direct – New Account message into the **Notification Address:** text field.
3. Click Submit.

**Figure 5 – Reset Password Page**




You should receive a notification email that looks like the following:


Clicking on the Set Password button will open a web page that links to the Change Password page. Accessing the page in this manner completes the password reset process.

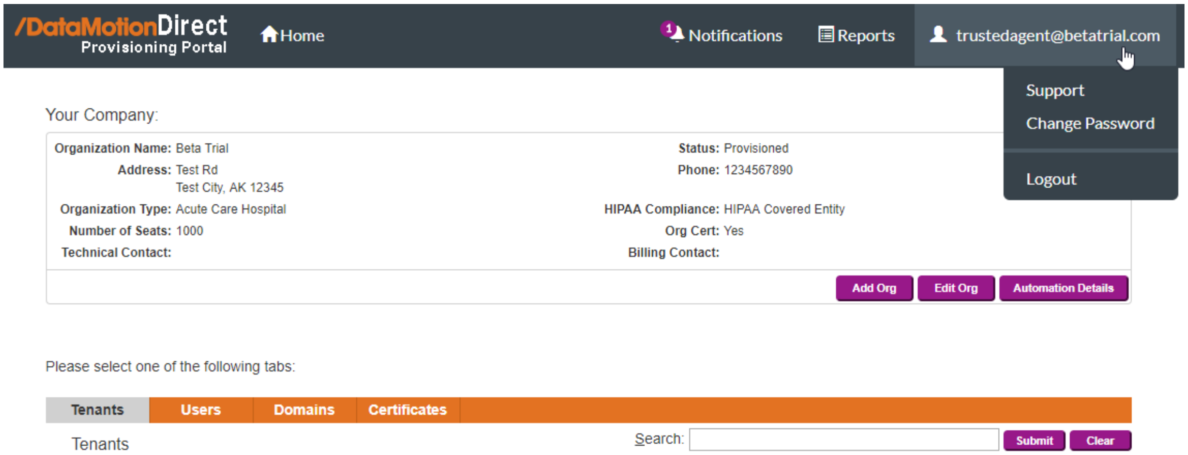
# NAVIGATION

## HOME

The following figure shows the components of the Home screen:

**NOTE: A TA user will see the Certificates tab, but an Administrator will not.**

**Figure 6 – Home screen controls**

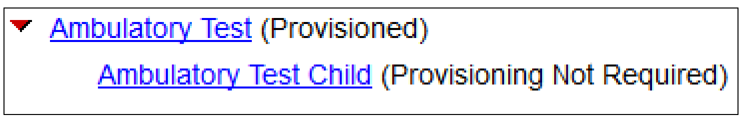



- **Home**: The link to the Home page which is always the initial page seen upon login.
- **Notifications**: The link to the Notifications page that contains web based notifications which appear if the TA or Admin selected web based notifications upon account creation.
- **Reports**: The link to the Reports page that contains options to run various reports for information regarding their HCO's activity. For information regarding these reports please see the Reports and Logging section on page 86.
- **Support**: The link to the Support page that contains various document templates to streamline the bulk import process as well as filling out the Declaration of Identity Document. (This link is contained in the drop-down shown when clicking on your username at the top right of the page).
- **Change Password**: This link takes you to the Change Password page where you can change your password as desired. (This link is contained in the drop-down shown when clicking on your username at the top right of the page).
- **Logout**: This link logs you out of the DPP. (This link is contained in the drop-down shown when clicking on your username at the top right of the page).
- **Add Org**: This button will direct you to the Create Organization page to create a new Tenant.
- **Tenants**: This tab contains all the tenants under the HCO. The hierarchy of the tenants is present here as well.

- **Users**: This tab displays a table of all the HCO's users that can be customized via drop-down.
- **Domains**: This tab displays a table of all the HCO's domains including the cert type, provisioning/validation status, and the date they were added.
- **Certificates**: This tab displays a table of all the HCO's certificates including the Subject the cert would belong to, the type of certificate, its status, the representing Trusted Agent, and the date the certificate was requested.

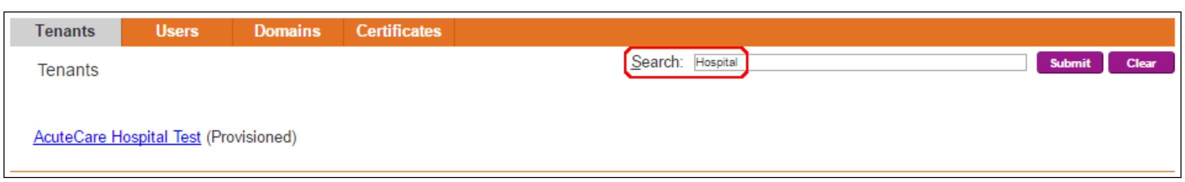
## TENANTS TAB

Every tenant company created through the DPP is created in a hierarchical structure which is displayed on this tab. Any organization that has an arrow to the left of its name contains additional tenants beneath itself in the hierarchy. The image below illustrates the general flow of how the hierarchy will continue to develop.




The only exception to the hierarchy is if there is only a single HCO in the company i.e. there are no additional tenants, then nothing at all will be displayed here (see Figure 6 for an example of this). On the other hand, if an HCO has a large number of tenants the hierarchical display may be overwhelming to search through. To make that process easier a search box is available to narrow down the visible list of tenants based on keywords. The search box searches for exact matches, so if a word such as "Hospital" is entered then any tenant with that word in its name will be listed.

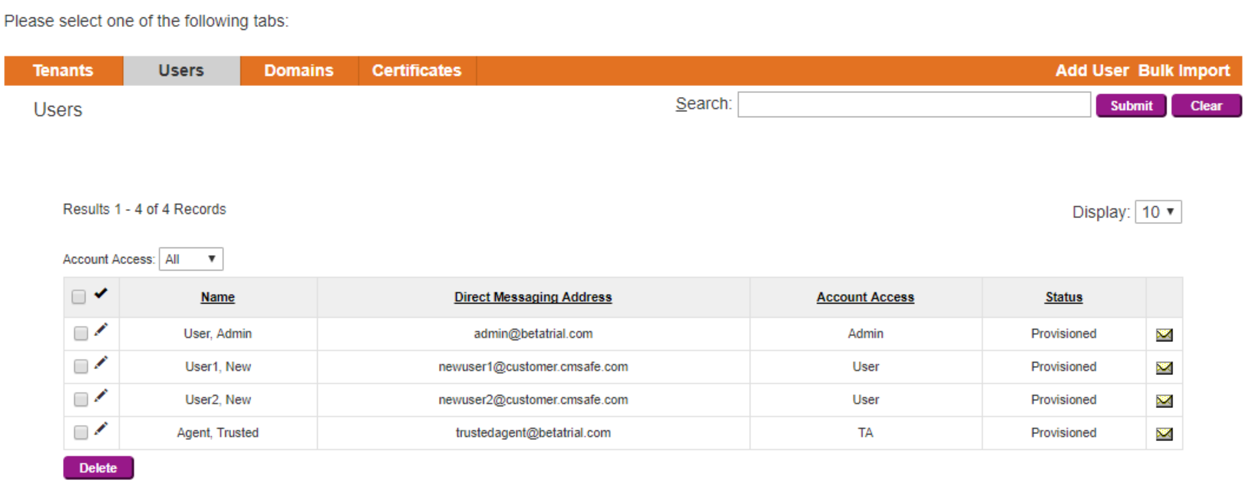
**Figure 7 – Tenants Tab**




## USERS TAB

All Direct User provisioning performed on the DPP is accomplished using the features provided on this tab. The table presents general user information including the current **Status** of a user in regard to validation or provisioning. When accessed a Trusted Agent or Administrator will be provided the following capabilities:

**Figure 8 – Users Tab**



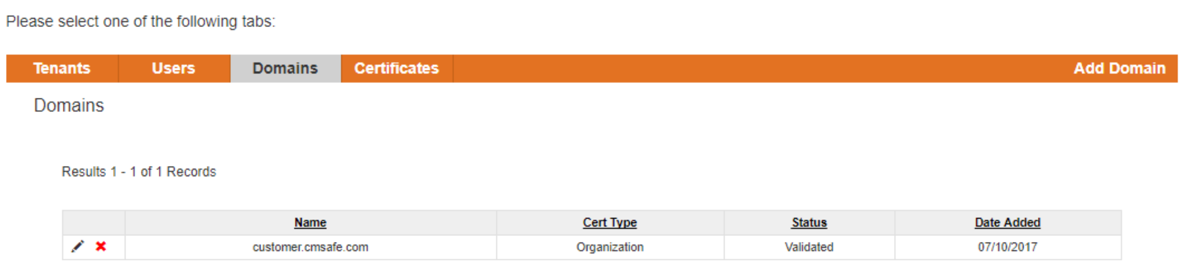

- **Search**: For tenants that possess a large number of users, the search bar can be used to filter the result list displayed in this tab.
- **Account Access**: This drop-down will display either All users, TA users, Admin users, or simply Users (which in this case are those who are Direct users on the system but lack any administrative functionality).
- **Display**: This drop-down will display anywhere from 10, 25, 50, or All users contained within a company at once on the screen.
- **Add User**: (for detailed information see the User Provisioning section).
- **Bulk Import**: (for detailed information see the *Provisioning Multiple Direct Users* section).
- **Delete User**: (In the unnamed column click the checkbox next to a user and then click the **Delete** button at the bottom of the page. A pop up will appear asking for confirmation, for more information see the *Deleting Users* section).
- **Edit User**: The icon in the unnamed column, will allow changes to any fields regarding a user see the *Editing Users* for more information.
- **Re-send Notification**: The icon will show a secondary menu that provides options to send a retry notification to the intended user. See the *Re-Sending Notifications (Retry Provisioning)* section.

This tab is only visible to Trusted Agent user types for security and compliance purposes.

## DOMAINS TAB

This tab provides an overview of the available domains that are active for an HCO. The Cert Type column is particularly important to take note of since that tells the TA what type of certificate can be used to provision users for the domain. The **Status** column contains valuable information regarding the validation and provisioning state of a certificate. Adding additional domains to an HCO is only possible by using this tab's Add Domain link located on the right side of the header. This is a feature available to both TA and Admin user types.

**Figure 9 – Domains Tab**




- **Add Domain**: This link will take you to the Add Domain page (for further information on adding domains see the Adding and Validating a Domain section).
- **Delete Domain**: (The icon next to the Name column). Be certain to revoke any certificates attached to the domain before attempting to delete.
- **Edit Domain**: (The icon next to the Name column). Allows all aspects of a domain to be edited, including its name and certificate type.

## CERTIFICATES TAB

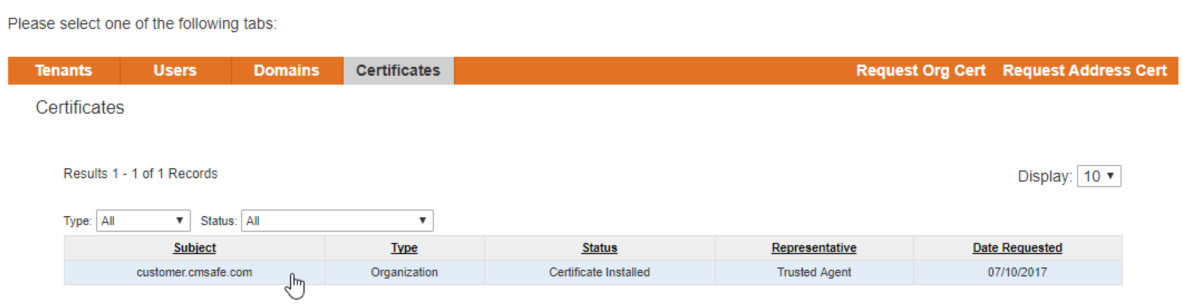
Every domain or user that has a certificate will be displayed in the table when this tab is being displayed. The table itself can be sorted based on the Type of certificate which is either Patient, Address, or Organization (set to All by default) using the appropriate drop-down. The table's display can be narrowed further via the Status drop-down which contains a list of all possible certificate statuses (set to all by default) which include the following:

- Request Rejected
- Awaiting Validation
- Revocation Requested
- Revocation Approved
- Revoke Failed 1
- Revoke Failed 2
- Revoke Failed 3
- Revoke Failed 4
- Revoke Failed Final
- Revoked
- Request Approved
- Certificate Generate Failure 1

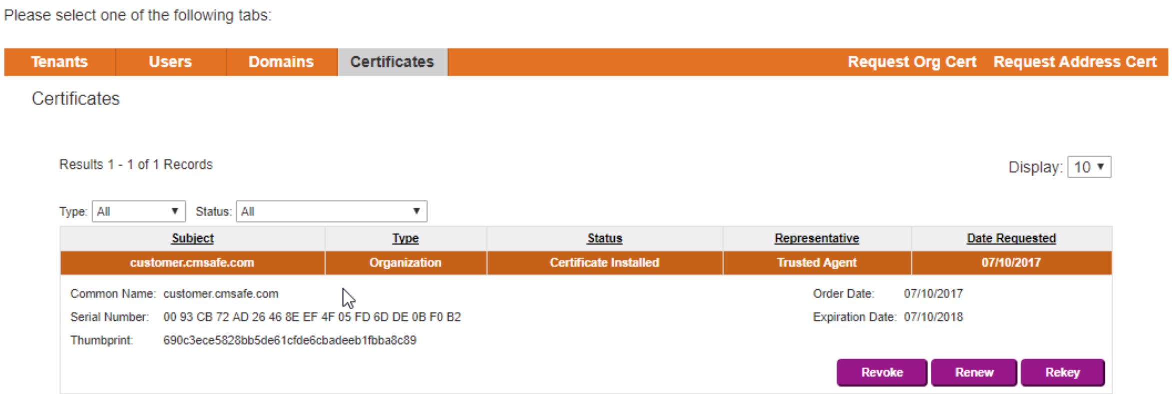
- Certificate Generate Failure 2
- Certificate Generate Failure 3
- Certificate Generate Failure 4
- Certificate Generate Failure Final
- Certificate Generated
- Certificate Install Failure 1
- Certificate Install Failure 2
- Certificate Install Failure 3
- Certificate Install Failure 4
- Certificate Install Failure Final
- Certificate Installed

All certificate actions that can be taken by TAs are performed using this tab, more specifically these actions are tied to the Revoke, Request Org Cert, and Request Address Cert links. The image *below* highlights these integral components.

**Figure 10 – Certificate screen controls**




The initial view of all certificates is displayed above. If a certificate is clicked on (you can click anywhere on the certificate as shown in the image above), the view will expand to show additional information and options.

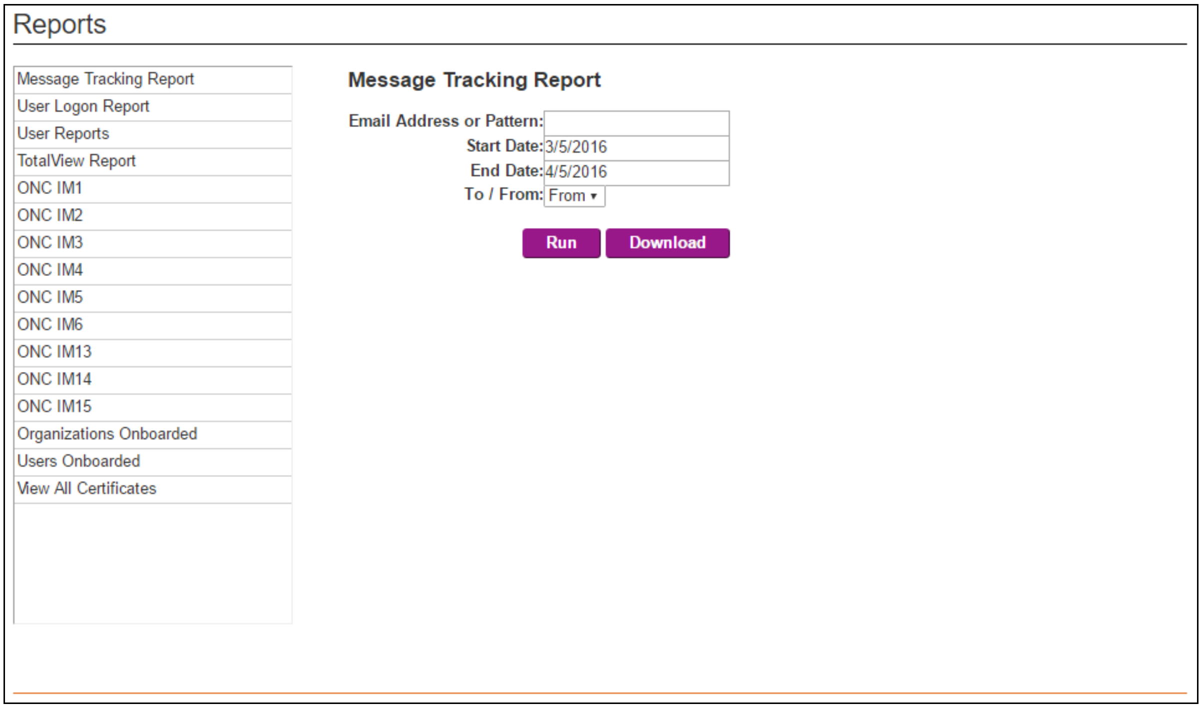



- **Revoke Certificate**: When clicked a pop-up will open that asks for user confirmation to submit the certificate for revocation (for additional information see the ***Revoking a Certificate*** section)
- **Subject**: The Subject is the domain of an Organization Certificate or the Direct Address of an Address or Patient Certificate.
- **Representative**: The TA named on the certificate.
- **Certificate Requests**: These links are used for requesting additional organizational or address certificates (for additional information see the ***Organizational Certificate Request*** and the ***Address Certificate Request*** sections).

## REPORTS

The following figure illustrates the components of the Reports screen:

**Figure 11 – Reports screen controls**



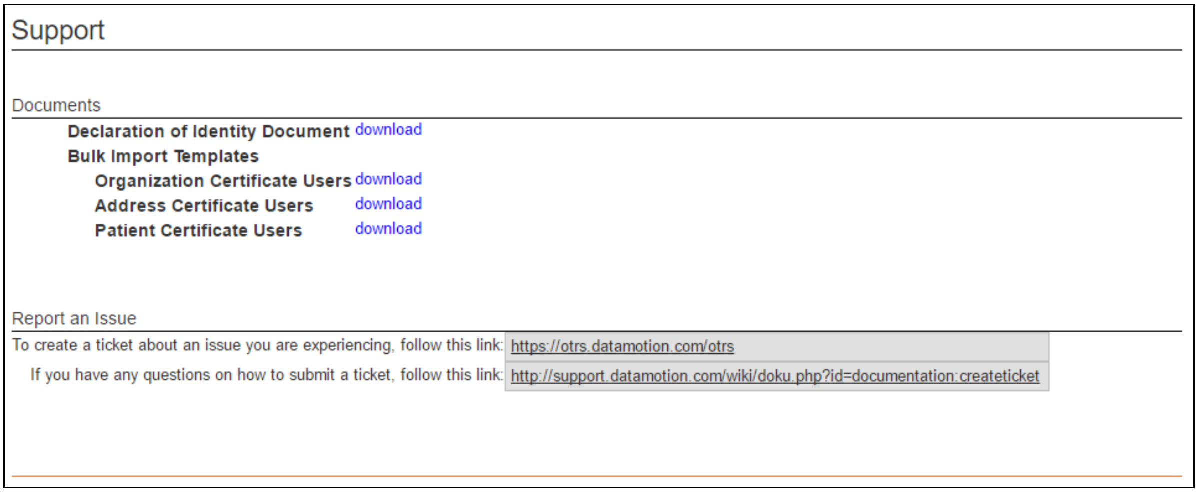

- Report Categories: On the left side of the page directly beneath Reports, is a list of the different types of reports available for the company.
- Export Options: The two buttons, Run or Download will either display the report within the browser (Run button) or download to a .CSV file (Download button).
- Report Dates: Every report with the exception of the User Reports and the View All Certificates reports will have a date range for collection including a Start and End Date to gather a particular range of data for the report.

**NOTE: The descriptions and the expected outputs of the various reports available for use on the DPP are described in a later section found *on page 86*.**

## SUPPORT

The following figure illustrates the components of the Support screen

**Figure 12 – Support Requests and Documentation**




- Documents: Links to download the appropriate templates that are required to perform bulk import tasks and provide the proper identity documentation whenever a DoID is requested.
- Report an Issue (Ticket Submission): instructions for submitting tickets for customer-related issues.

# 3
# Organizational Provisioning

## PROVISION A TENANT ORGANIZATION

As a company administrator (or Trusted Agent), you will be responsible for onboarding your tenant/children companies. The following sections describe the requirements for provisioning a tenant company.

### PREREQUISITES

Cancelling the provisioning process before it has been completed will cause an error with registration and delay the organization from beginning the exchange of Direct messages. For this reason, please have the following ready and completed before beginning the provisioning process:

**Table 2 – Prerequisites for registering an organization**

| Prerequisite | Reason |
|---|---|
| Declaration of Identity | This form should be filled out (by the TA applicant) in the presence of either and already validated TA, or a Notary public. This form is only necessary when creating a new TA. |
| Direct domain (or subdomain) | A Direct specific domain (or subdomain) is required for organizations that will request org certs. |
| Identification for the TA applicant | A new TA applicant must present identification to either an already validated TA or Notary public in order for the DoID to be signed. Information regarding that information must also be entered during the application process |

#### Government Issued ID Requirements

The validation process requires that a government issued ID be submitted if a Trusted Agent is being created. If you are not creating a Trusted Agent for the organization you can skip to the *Company Information* prerequisite on page 33.

In some cases, two IDs will be required for submission. It should be noted that only the Driver's License prompts the need for a second ID, which in itself is dependent on the state. A list of states requiring two IDs is listed below for convenience.

- Arkansas
- Arizona
- Kentucky
- Louisiana
- Massachusetts
- Maine
- Minnesota
- Montana
- New Jersey
- New York
- Oklahoma
- Washington

If the Driver's License being used for validation is from one of these states please have a second government issued ID available. A passport is the ideal option for the second choice since a passport is not tied to a state. If a passport is not available then a State ID will be required as the second ID for states listed above.

A State ID is generally considered a Non-Driver's Identification Card, and is issued by an office under the state's Department of Transportation. For every state a Department of Motor Vehicles office will suffice. The actual process of acquiring the ID varies from state to state and does include a fee of some sort.

In general, the acquisition of this ID will require an identification process performed by the DMV. A birth certificate and social security card are almost universally required in every state along with additional identification materials. Applications for these IDs are performed in person as well.

**NOTE: If it is at all possible the Passport option is the ideal choice to fill in for the first ID. This is because the Passport option will not prompt the submission of a second ID at all during the provisioning process or when adding Direct Users covered by Address Certificates or Trusted Agents.**

## NOTE Regarding Photo ID Submission

If during the process to add a Direct User covered by an Address Certificate or a Trusted Agent it might be the case that the user being added does not have a second photo identity that satisfies the choices in the Photo ID Type drop-down. Should this be the case

DataMotion will allow for the submission of the Driver's License a second time. Just select the State ID in the drop-down and enter the same information for the Driver's License again.

### Company Information

To ensure quick validation during the provisioning process, the company's business license, EIN, or NPI will have to be entered. Only one is required for submission, so whichever of the three items is the easiest to provide for the organization being added should be on hand in advance.

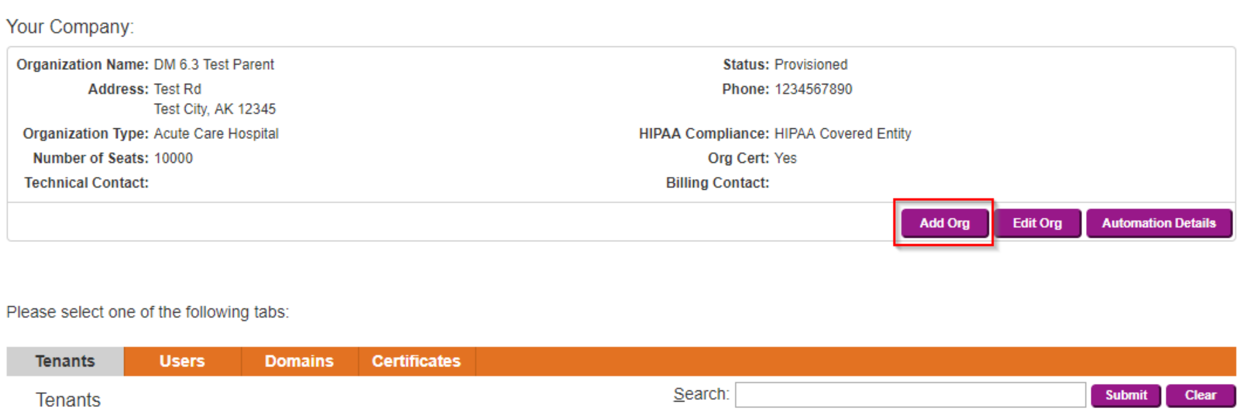
## CREATE ORGANIZATION

Creating a Healthcare Organization is the first step in the process to fully provision an HCO to have access to DataMotion Direct Secure Messaging. For first time users this step will actually have already been completed by a DataMotion Officer.

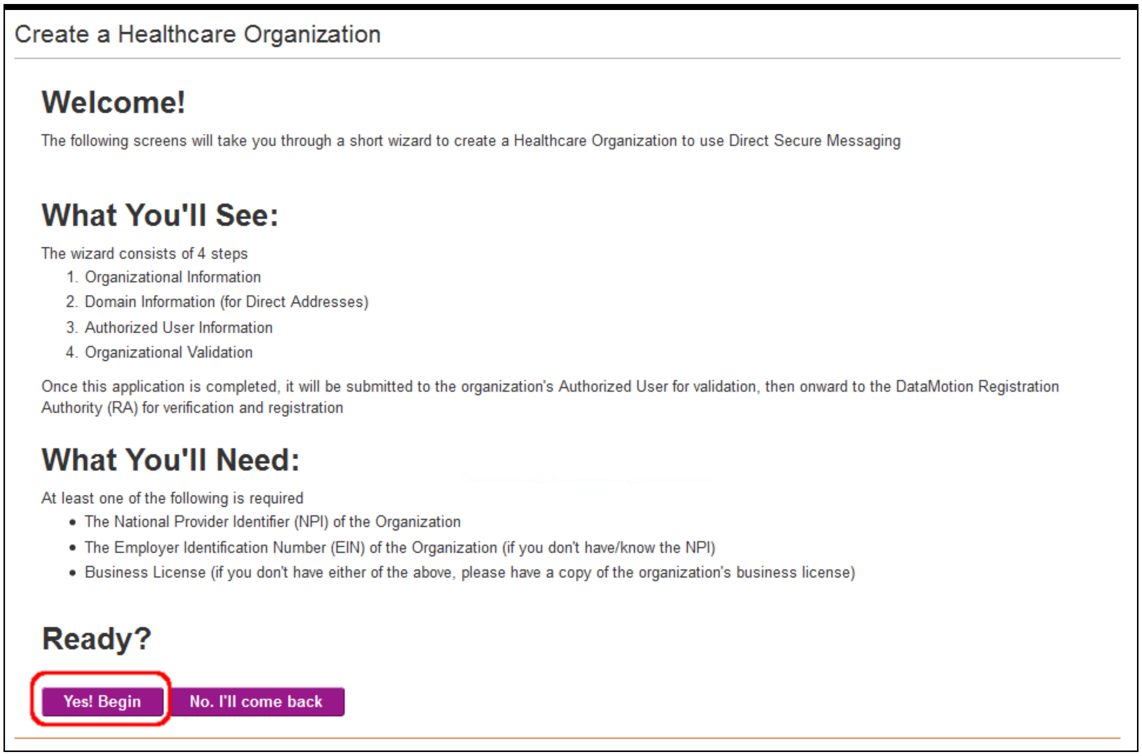
**For tenants of DataMotion only: To simply complete registration for your own company, begin with the *Register Organization* step *below*.**

On the "Home" screen, select the host company for the new tenant company to be added. This will most likely be your company. Then select the Add Org button to begin the application process.

**Figure 13 – Adding a tenant company**



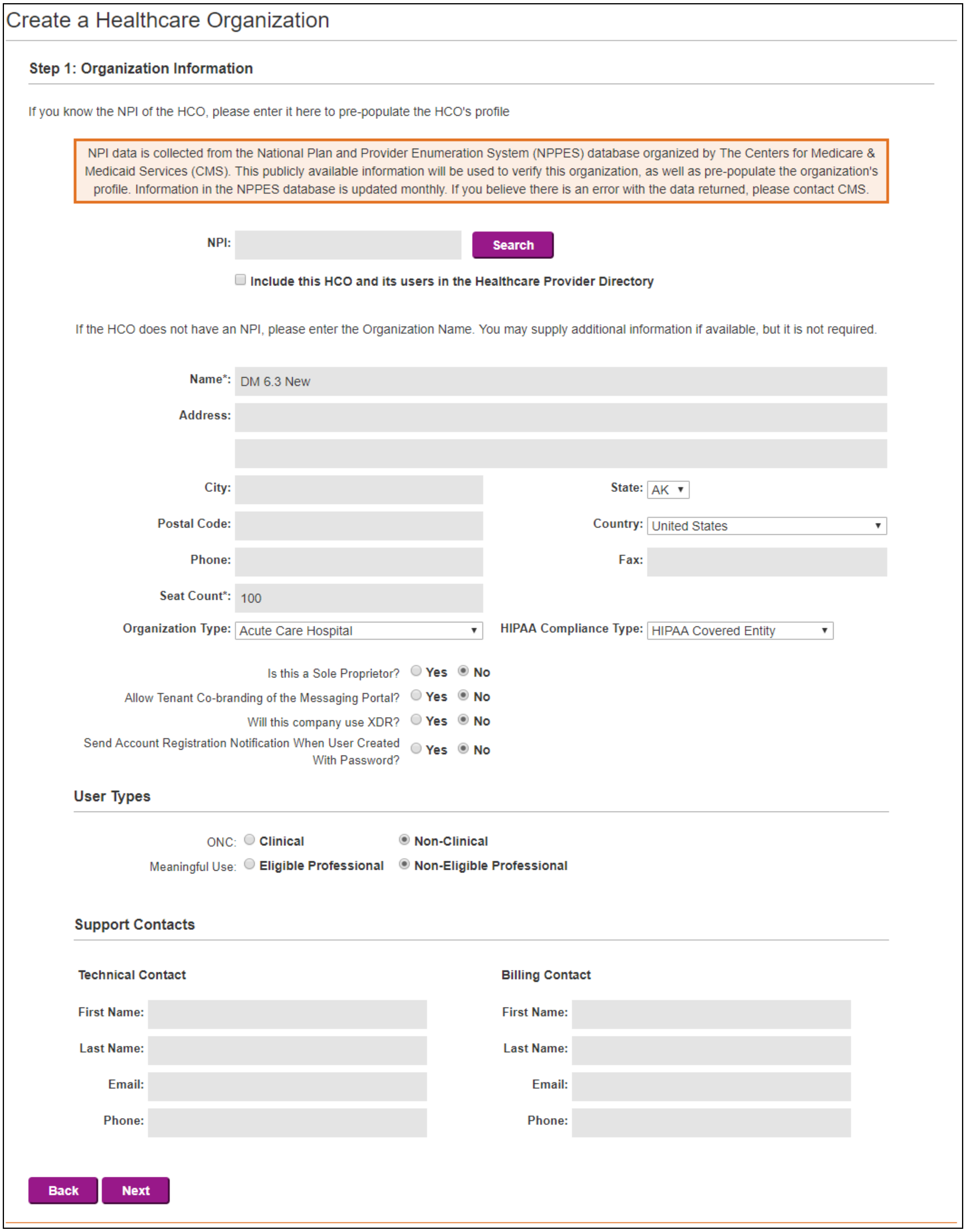

1. The **Create a Healthcare Organization** page will be displayed.




2. Read this page carefully, and gather all of the materials listed under the **What You'll Need** section.
3. Click the **Yes! Begin** button to start *Step 1: Organization Information*.

## Step 1: Organization Information (Create Organization)

**Figure 14 – Create a Healthcare Organization Step 1 (Organization Information)**



Create a Healthcare Organization

**Step 1: Organization Information**

If you know the NPI of the HCO, please enter it here to pre-populate the HCO's profile

NPI data is collected from the National Plan and Provider Enumeration System (NPPES) database organized by The Centers for Medicare & Medicaid Services (CMS). This publicly available information will be used to verify this organization, as well as pre-populate the organization's profile. Information in the NPPES database is updated monthly. If you believe there is an error with the data returned, please contact CMS.

NPI: [ ] **Search**

☐ **Include this HCO and its users in the Healthcare Provider Directory**

If the HCO does not have an NPI, please enter the Organization Name. You may supply additional information if available, but it is not required.

**Name*:** DM 6.3 New
**Address:**
**City:** **State:** AK
**Postal Code:** **Country:** United States
**Phone:** **Fax:**
**Seat Count*:** 100
**Organization Type:** Acute Care Hospital **HIPAA Compliance Type:** HIPAA Covered Entity

Is this a Sole Proprietor? ○ Yes ◉ No
Allow Tenant Co-branding of the Messaging Portal? ○ Yes ◉ No
Will this company use XDR? ○ Yes ◉ No
Send Account Registration Notification When User Created With Password? ○ Yes ◉ No

**User Types**

ONC: ○ Clinical ◉ Non-Clinical
Meaningful Use: ○ Eligible Professional ◉ Non-Eligible Professional

**Support Contacts**

**Technical Contact**
First Name:
Last Name:
Email:
Phone:

**Billing Contact**
First Name:
Last Name:
Email:
Phone:

**Back** **Next**

1. If you know the NPI of the HCO you are trying to add, enter it into the NPI field to pre-populate most of the information on this page.
   » If not, then manual input of the data will be required.
2. Enter the information of the HCO to be added into the appropriate fields. Only the Name and Seat Count fields are required.
   » It is recommended that you input as much information for as many fields as possible to make additional actions easier in the future.
   » User Types: These define the types of users within the organization, for ONC/MU2 reporting. If the organization consists of both Clinical and Non-Clinical users, select Clinical. Similarly, if the organization consists of both EP (Eligible Professionals) and Non-EP, select EP.
   » Support Contacts: The information in this section is optional; however, in the case that any technical or billing issues arise, contact information here will greatly expedite solving any issues.

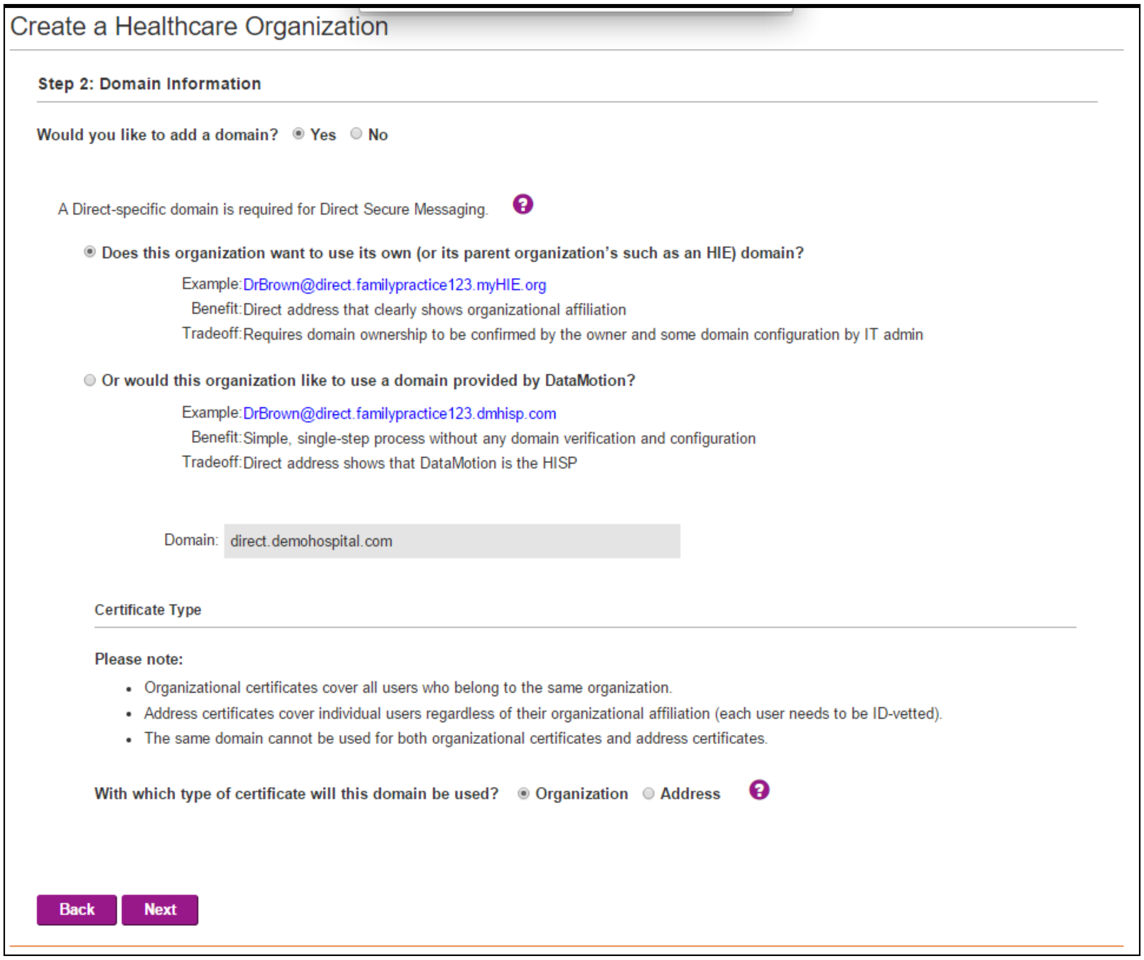
**NOTE: If the company must have its users entered into the HPD, select the checkbox to the left of** Include this HCO and its users in the Healthcare Provider Directory**. This can be changed later, see the** *Editing an HCO* **section for details.**

3. Select Next, and proceed to Step 2: Domain Information.

**NOTE: Clicking the Next button will commit the creation of this HCO to the DPP. This means that the registration process for this organization must be completed with the Name that it was given in this step. Please ensure that the name of this organization is correct to avoid having to restart this process.**

## Step 2: Domain Information (Create Organization)

**Figure 15 – Create a Healthcare Organization Step 2 Domain Information**




1. Select Yes or No to add a domain to the DPP. Selecting Yes will display the options available.

**NOTE: It is highly advised to select Yes at this step and create a domain. No certificates can be added without a domain and this is the easiest time to add one.**

2. Decide whether or not you want to use a domain of your own choosing by selecting the first radio button, or if you want to use a DataMotion domain by selecting the second radio button.

**NOTE: If you choose to use a DataMotion domain it will not be possible to select Organization as the Certificate Type.**

3. Enter the name of the domain you want in the Domain field.

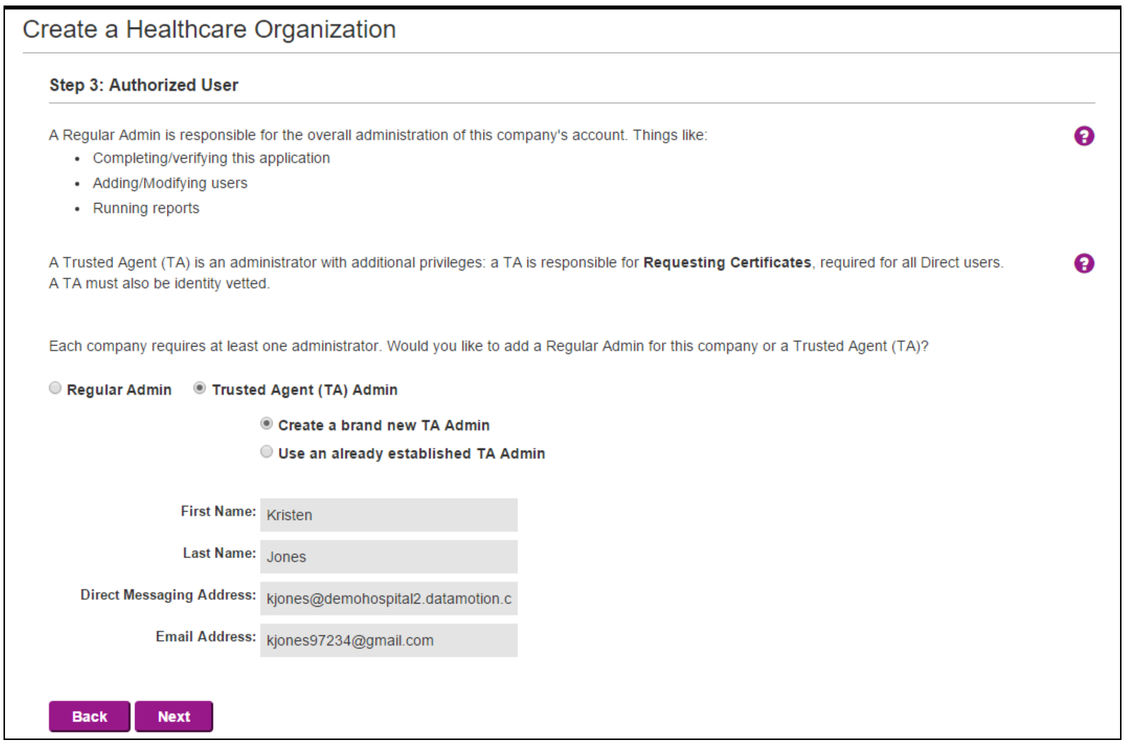
4. Select the Certificate type, either Organization or Address is available.

5. Click Next to continue.

## Step 3: Authorized User (Create Organization)

When creating a company for the first time it is important to note that a company created without a Trusted Agent as the authorized user will be unable to perform certificate requests. It will also not be possible for that company to acquire a Trusted Agent on its own and someone within that company will have to request the parent HCO to initiate the *Creating a New Trusted Agent* process on their behalf. If for any reason this is an issue for the parent HCO then DataMotion itself will have to be contacted, and a DataMotion Officer will have to initiate the process.

**Figure 16 – Create a Healthcare Organization Step 3 Authorized User**



Create a Healthcare Organization

**Step 3: Authorized User**

A Regular Admin is responsible for the overall administration of this company's account. Things like:
- Completing/verifying this application
- Adding/Modifying users
- Running reports

A Trusted Agent (TA) is an administrator with additional privileges: a TA is responsible for **Requesting Certificates**, required for all Direct users. A TA must also be identity vetted.

Each company requires at least one administrator. Would you like to add a Regular Admin for this company or a Trusted Agent (TA)?

Regular Admin    Trusted Agent (TA) Admin

Create a brand new TA Admin
Use an already established TA Admin

First Name: Kristen
Last Name: Jones
Direct Messaging Address: kjones@demohospital2.datamotion.c
Email Address: kjones97234@gmail.com

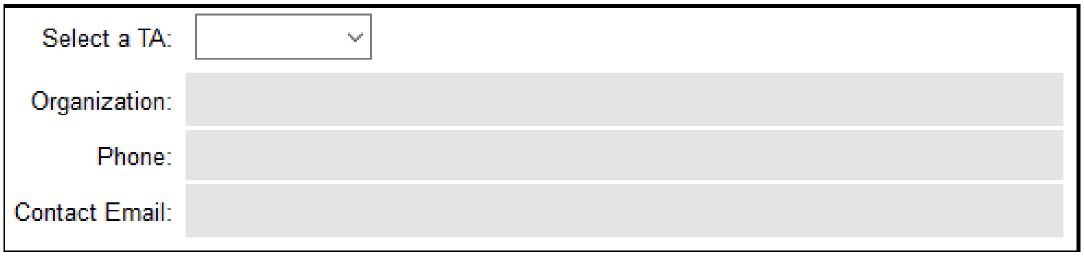
Back  Next

The Authorized User will be tasked with performing administrative and TA functions for the HCO.

1. Select either the Regular Admin or Trusted Agent (TA) Admin radio buttons.
   » Please note that if Regular Admin is selected the HCO will not have a Trusted Agent. This means that the HCO will be unable to perform any certificate requests and be unable to create a TA without the assistance of a DataMotion Officer or a TA from a parent company.

   **NOTE: As a result of this it is critical that a TA be added at this step.**

2. If TA Admin was selected in the previous step, select either **Create a brand new TA Admin** or **Use an already established TA Admin**.
   - Selecting **Create a brand new TA Admin** user at the HCO will prompt the creation of a new TA which requires the steps listed in the Step 3: Authorized User (Register Organization) section to be performed.
   - Selecting **Use an already established TA Admin** from an existing HCO will prompt the following:

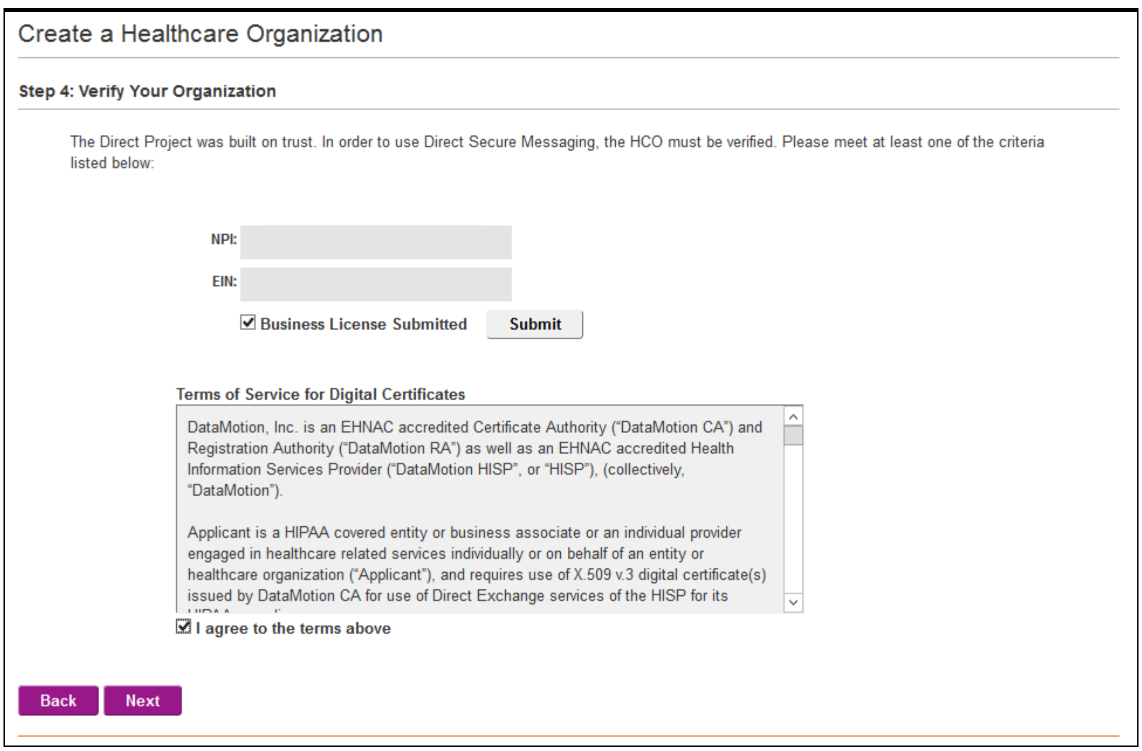



   - Use the **Select a TA**: drop-down to choose the TA for the HCO. The **Organization**, **Phone**, and **Contact Email** will be auto populated upon selection.

3. Click Next to move to Step 4: Verify Your Organization (Create Organization)

## Step 4: Verify Your Organization (Create Organization)

**Figure 17 – Create a Healthcare Organization Step 4 Verify Your Organization**

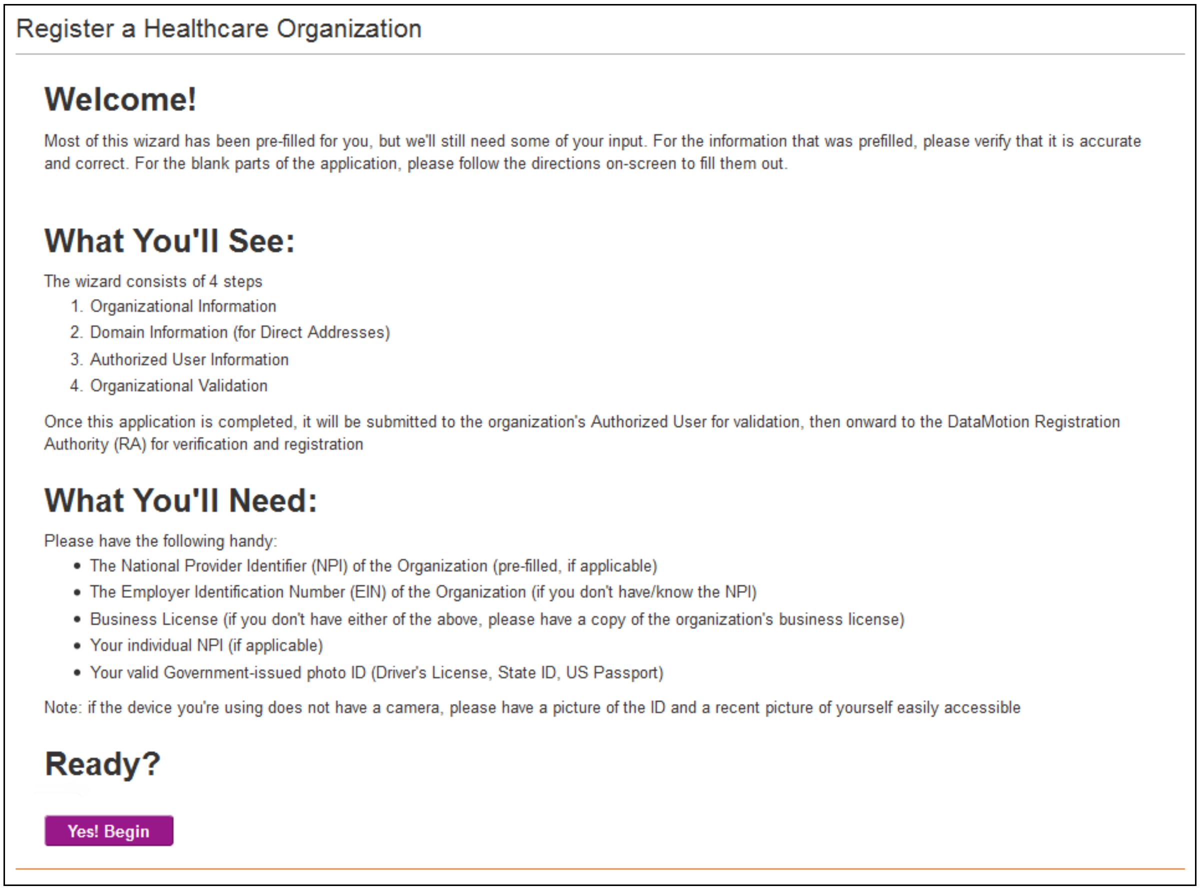


1. Enter either the NPI, EIN, or Business License of the organization being registered.
   » Submitting the Business License will open an email client on your computer when the Submit button is clicked. Attach the organization's Business License to this email and send it to the designated party at DataMotion. Once that task is completed, click the **Business License Submitted** checkbox.
2. Click the **I agree to the terms above** checkbox.
3. Click Next to complete the process.

## REGISTER ORGANIZATION

Successful creation of an HCO will send a notification email to the TA that was designated during the creation process that informs them an HCO requires registration. If a new TA was created for this HCO then that TA will have to create a password (see the ***Creating Your Login Credentials*** section) before they are brought to the appropriate registration page. In either case successful login will navigate the TA to the Register a Healthcare Organization page and display a page outlining the general procedure and the information you must have prepared in order to meet the requirements of the registration process. If you do not have all of the required information being asked for on the page, it will not be possible to complete the process.

**Figure 18 – Register a Healthcare Organization Process**


Register a Healthcare Organization

## Welcome!

Most of this wizard has been pre-filled for you, but we'll still need some of your input. For the information that was prefilled, please verify that it is accurate and correct. For the blank parts of the application, please follow the directions on-screen to fill them out.

## What You'll See:

The wizard consists of 4 steps

1. Organizational Information
2. Domain Information (for Direct Addresses)
3. Authorized User Information
4. Organizational Validation

Once this application is completed, it will be submitted to the organization's Authorized User for validation, then onward to the DataMotion Registration Authority (RA) for verification and registration

## What You'll Need:

Please have the following handy:

- The National Provider Identifier (NPI) of the Organization (pre-filled, if applicable)
- The Employer Identification Number (EIN) of the Organization (if you don't have/know the NPI)
- Business License (if you don't have either of the above, please have a copy of the organization's business license)
- Your individual NPI (if applicable)
- Your valid Government-issued photo ID (Driver's License, State ID, US Passport)

Note: if the device you're using does not have a camera, please have a picture of the ID and a recent picture of yourself easily accessible

## Ready?

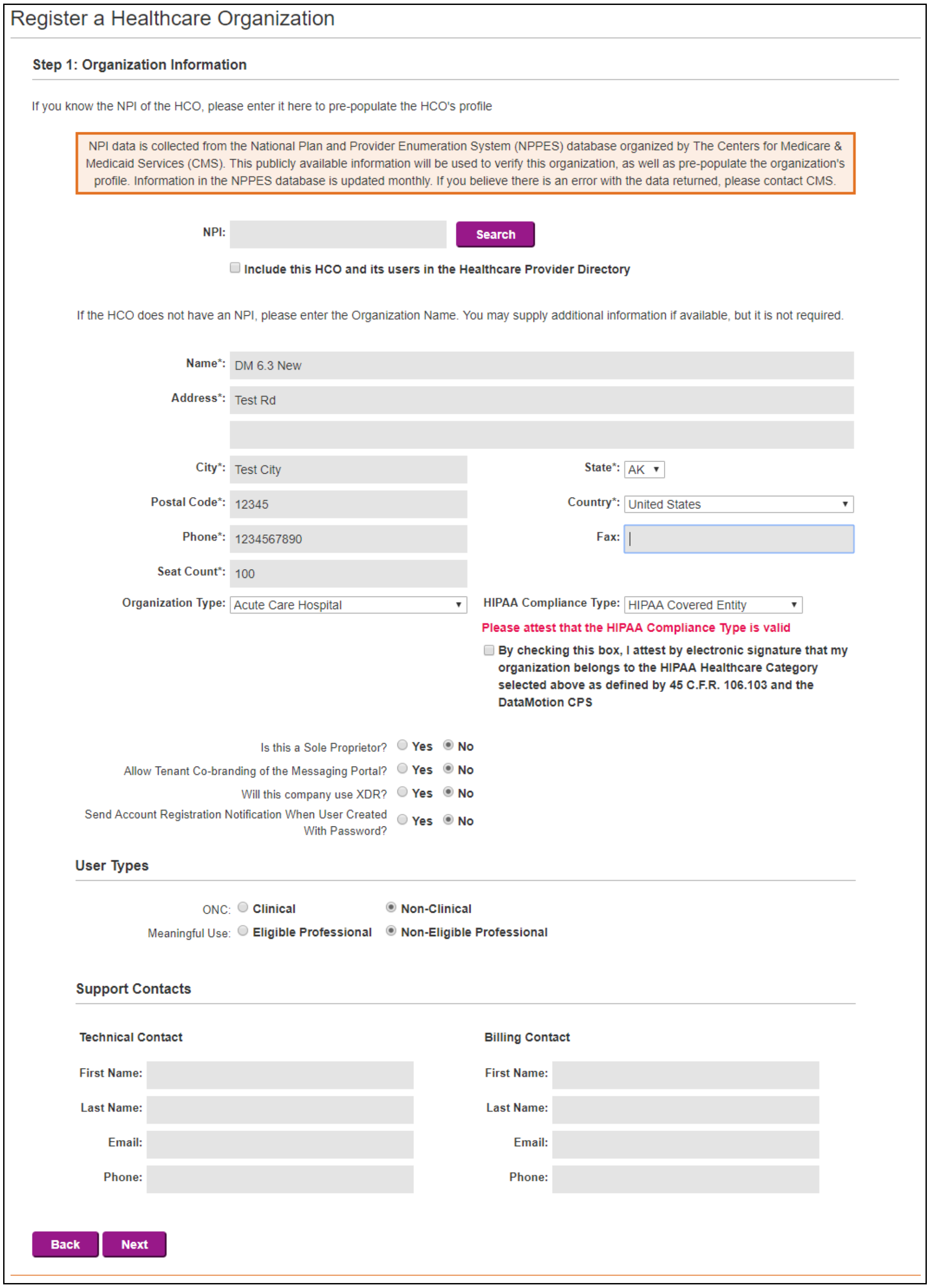
Yes! Begin

Please note that clicking the Yes! Begin button will prompt the acceptance of a Terms of Service. Once the terms are agreed to, the registration process will start.

### Step 1: Organization Information (Register Organization)

The Name and Seat Count fields should already have been entered during the Create Organization process.

**Figure 19 – Register a Healthcare Organization Step 1 Organization Information**




1. If the NPI was not previously entered or there are still fields left empty, input accurate information for the remaining fields marked with an * symbol.

2. Select the **Organization Type** of the HCO. You can select either Acute Care Hospital, Ambulatory Practice/Entity, Non-hospital Clinical Lab, or Other Health Care Related Organization.

3. Select the **HIPAA Compliance Type** of the HCO. You can select either HIPAA Covered Entity, HIPAA Business Associate, or Other HIPAA Entity.

**NOTE: This decision must be confirmed and it will not be possible to proceed without clicking the checkbox as shown in the image above.**

4. Choose if the HCO is a Sole Proprietor.

5. Decide if the HCO will be allowed to have its tenants cobrand the Direct Messaging Portal.

6. Choose if the HCO will use XDR.

7. Select the User Types present within the HCO.
    - User Types: These define the types of users within the organization, for ONC/MU2 reporting. If the organization consists of both Clinical and Non-Clinical users, select Clinical. Similarly, if the organization consists of both EP (Eligible Professionals) and Non-EP, select EP.

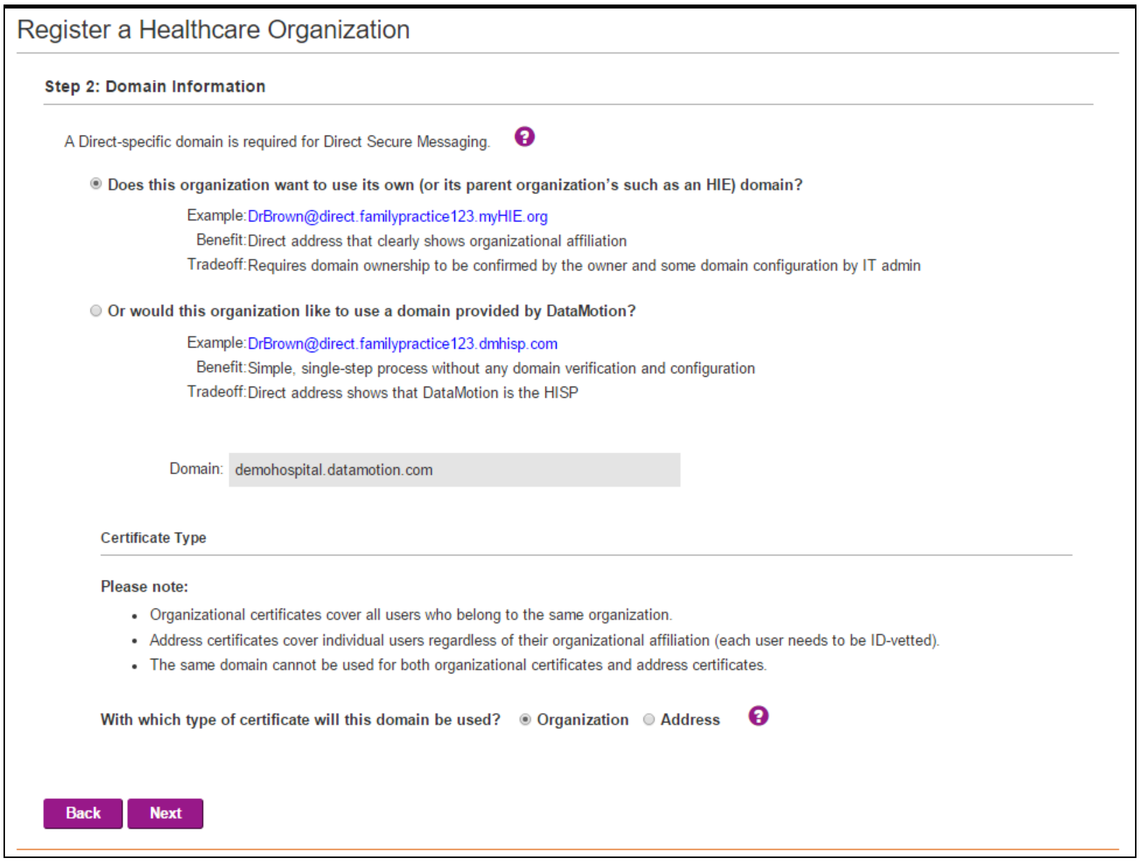
8. Input information for the HCO's Support Contacts if applicable.
    - This step is not required, however, in the case that any technical or billing issues arise, contact information here will greatly expedite solving any issues.

9. Click Next to proceed to Step 2: Domain Information (Register Organization)

## Step 2: Domain Information (Register Organization)

Domain information could have been entered during the Create Organization process. It is possible to change this information now if desired. It is not advised to change this information however if a new TA or Admin user was created during the Create Organization process as that user was most likely created using the domain information being displayed.

**Figure 20 – Register a Healthcare Organization Step 2 Domain Information**




1. Select Yes or No to add a domain to the DPP. Selecting Yes displays the options available.

2. Decide whether you want to use a domain of your own choosing by selecting the first radio button, or if you want to use a DataMotion domain by selecting the second radio button.

**NOTE: If you choose to use a DataMotion domain it will not be possible to select Organization as the Certificate Type.**

3. Enter the name of the domain you want in the Domain field.

4. Select the Certificate type, either Organization or Address is available.

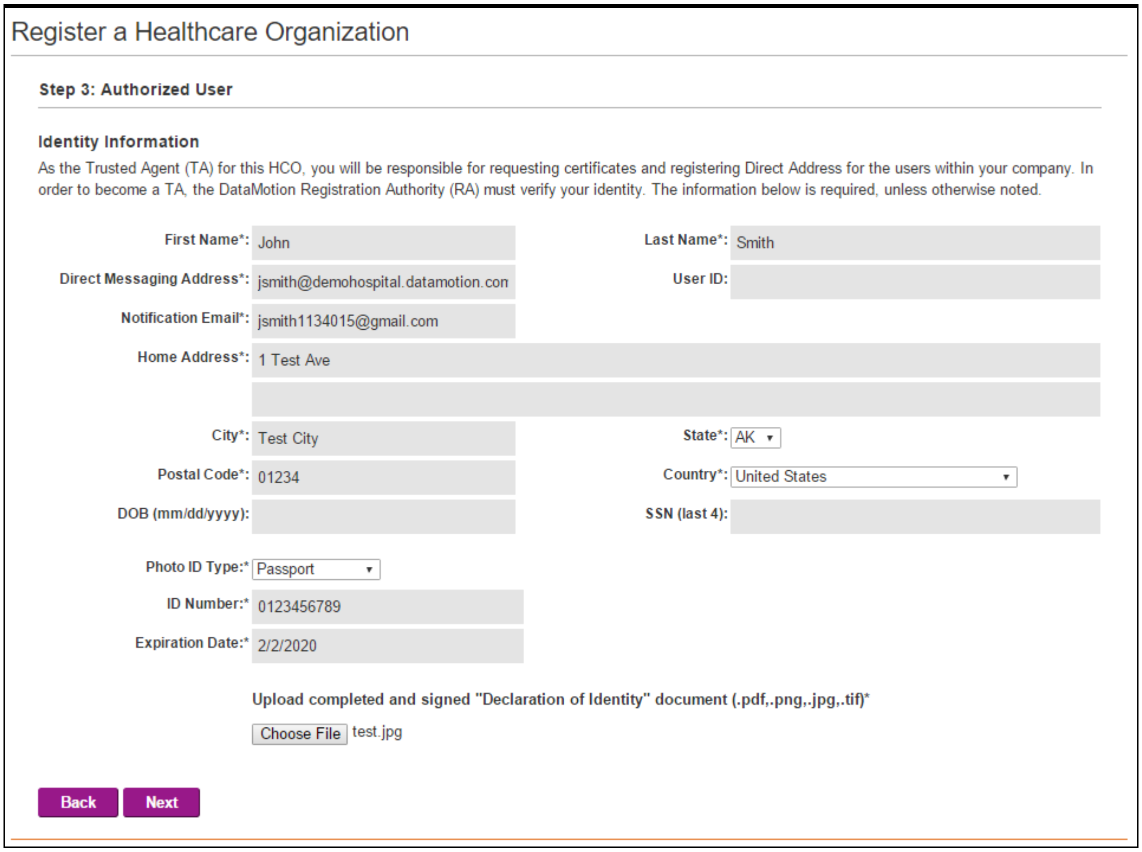
5. Click Next to continue to Step 3: Authorized User (Register Organization).

## Step 3: Authorized User (Register Organization)

This step of the process varies depending on the decision made during the Step 3: Authorized User portion of the Create Organization process. If the decision was to have a TA assigned to the HCO being created then this entire step is not required. If a new TA was to be created for this HCO, then this step must be followed in its entirety.

**Note: In the provisioning process, a TA user account cannot be created with an active Direct address i.e. the Direct Address created in this step is only there as a placeholder and not attached to a certificate.**

**Figure 21 – Register a Healthcare Organization Step 3 Authorized User**




1. Enter accurate information into all fields on this page that have a * symbol.
   - » The Photo ID Type drop-down contains the types of ID that are acceptable for submission which are a Driver's License, Passport, or State ID.
   - » In some cases, a second ID may be required depending on which Photo ID Type was selected. This only occurs for certain states. The Government Issued ID Requirements section contains information regarding this.

**NOTE: Provide the Photo ID Type, State (if applicable, the Passport option does not have this choice), ID Number, and Expiration Date.**

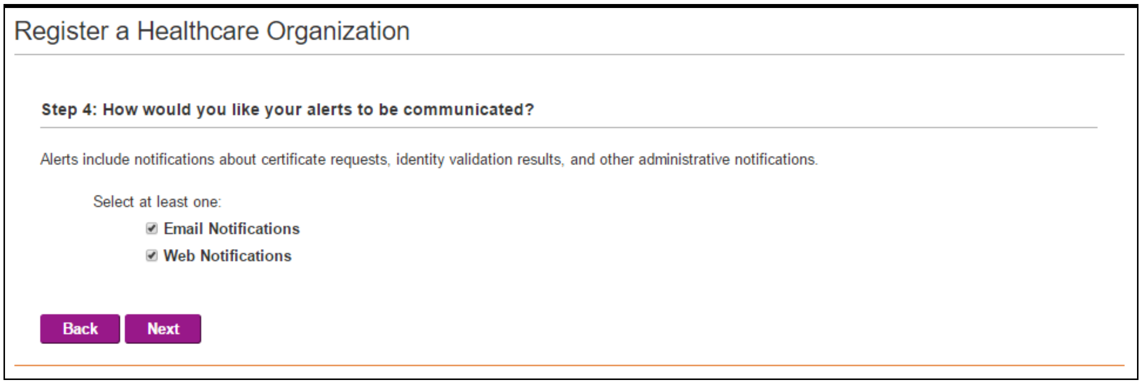
2. Upload the signed DoID which must be in one of the formats specified on the page (.pdf, .png, .jpg, and .tif are currently accepted).

3. Click Next to proceed to Step 4: How would you like your alerts to be communicated?

**NOTE: Ensure that the DoID being submitted is fully accurate and validated (signed by a notary or existing Trusted Agent) before clicking the Next button. If not, then the entire process will have to be restarted beginning with the Create Organization step.**

## Step 4: How would you like your alerts to be communicated?

**Figure 22 – Register a Healthcare Organization Step 4 Communication Alerts**



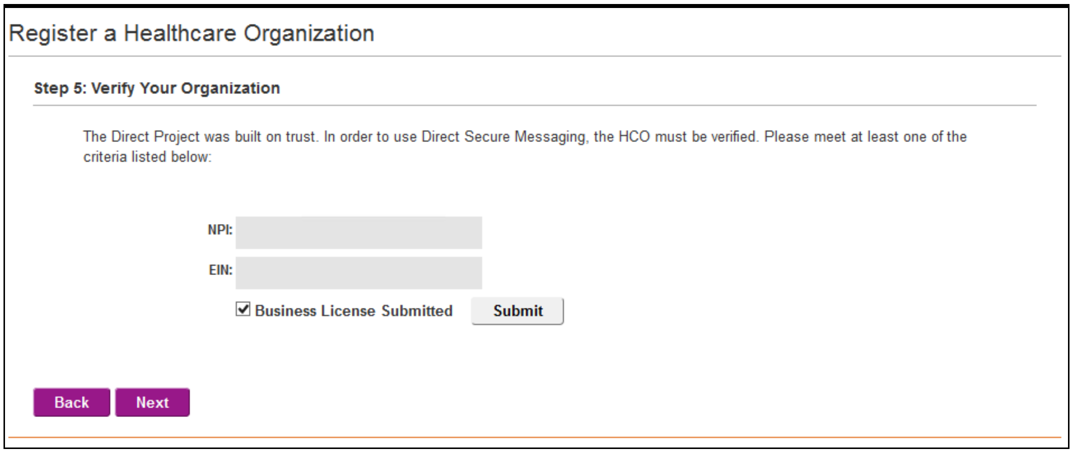

1. Select how notifications should be received. It is possible to select both.
   - » Email Notifications will send all relevant notifications to the email address provided during Step 3: Authorized User (Register Organization).
   - » Web Notifications will submit all notifications to the web UI itself.

2. Click Next to proceed to Step 5: Verify Your Organization.

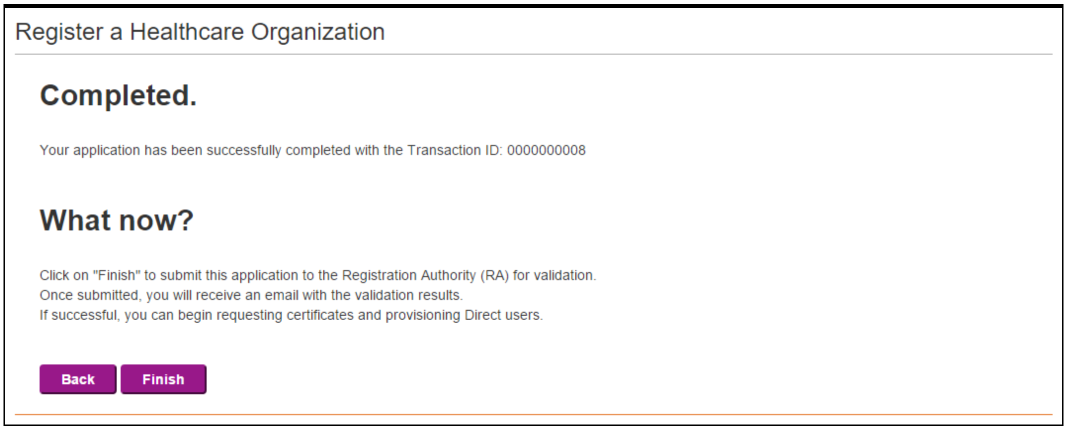
## Step 5: Verify Your Organization (Register Organization)

The information provided during this step should match the information that was provided during Step 4: Verify Your Organization (Create Organization) of the Create Organization process. It is possible to change the information during this step if desired, however it is not advised. The reason for this being that when the organization is reviewed by a DataMotion Officer it could cause some confusion to as why there is a discrepancy present in this step if the information provided is not congruent in both steps (i.e. an NPI is entered here, when a business license was submitted in the prior steps). This does not mean that the registration will be a failure, but it could cause delays in the validation process.

**Figure 23 – Register a Healthcare Organization Step 5 Verify Your Organization**




1. Enter either the NPI, EIN, or Business License of the organization being registered.
   - » Submitting the Business License will open an email client on your computer when the Submit button is clicked. Attach the organization's Business License to this email and send it to the designated party at DataMotion. Once that task is completed, click the **Business License Submitted** checkbox.
2. Click Next to complete the application.




3. Click the Finish button to submit the registration to DataMotion for validation.

**NOTE: If your company has Awaiting Validation next to Status, it is still waiting for a DataMotion Officer to approve the company validation. The Status will change to Provisioned when the company is approved.**

**NOTE: Once an Organization is validated by a DM Officer, only the co-branding and the contact information can be edited. Please ensure that all information is properly entered into the portal before selecting the Submit button.**

# 4
# Trusted Agent Actions

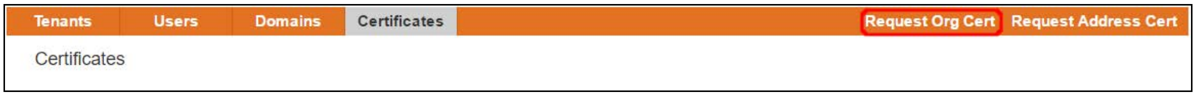
**All Actions described throughout this chapter are only available to Trusted Agents on the DPP. A normal Admin user cannot perform these tasks with only Editing Users as an exception (for information see the *Editing Users* section *on page 54*).**

## CERTIFICATE REQUESTS

When a TA has been successfully created, they can request certificates via the **Certificates** tab. Users must have a valid Direct address in order to obtain a certificate. This will require a domain designated to be covered under an Organization Certificate or Address Certificate. If your company does not have any domains at this time, see the Adding and Validating a Domain section. If there are no domains it will not be possible to apply a certificate.

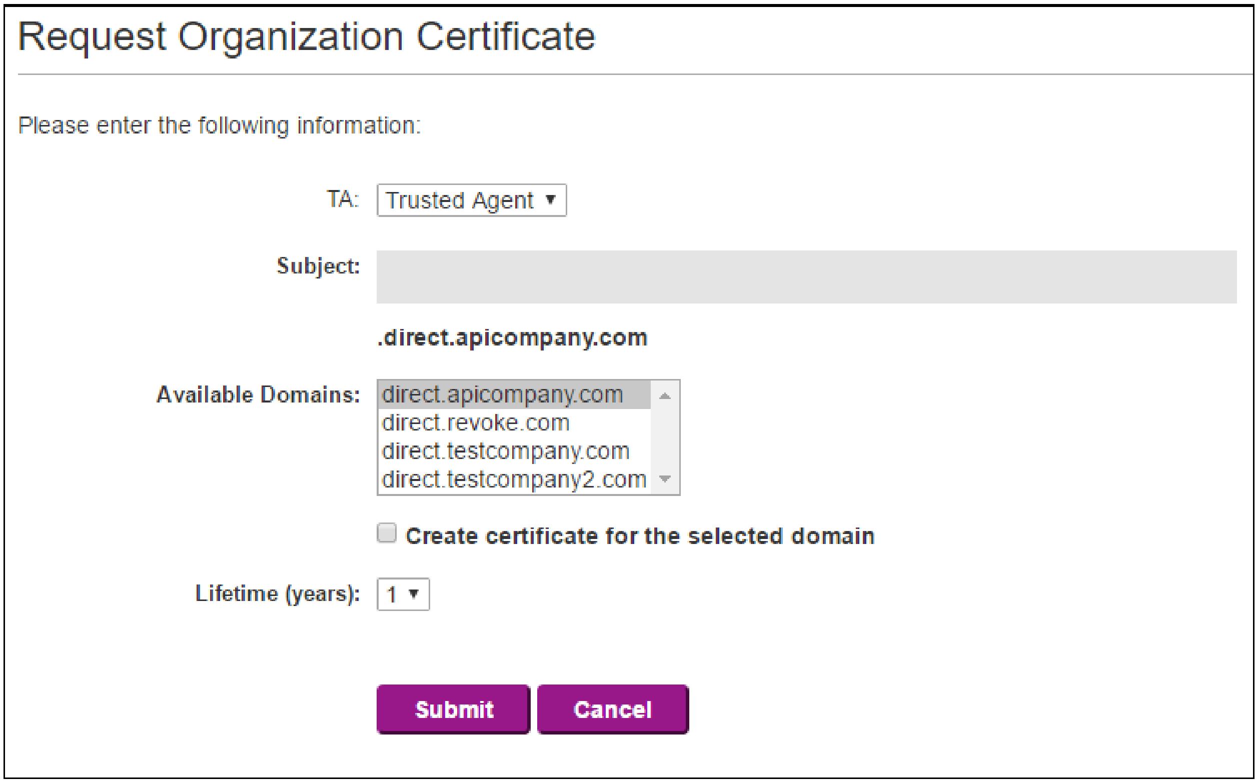
### ORGANIZATIONAL CERTIFICATE REQUEST

Requesting an organizational certificate requires a TA that is either assigned to you, or you have a validated TA of your own. The domain that is going to be used for the organizational certificate must also be validated in order to make this request. For information on validating the domain see the Adding and Validating a Domain section on page 80. To make the request itself, use the **Request Org Cert** field below.




**NOTE: If the domain has not been validated successfully and there is no TA user, the fields to make the request will be inaccessible.**

**Figure 24 – Request an Organization Certificate**




1. On the Home page, click the **Certificates** tab, then press the **Request Org Cert** link.

   **NOTE: If you have no Active Domains, (i.e. you do not have any organizations which have had a domain validated during the provisioning process or added separately) then see the Adding and Validating a Domain section for information on how to separately add domains in order to use organizational certificates.**

2. Select which TA will be responsible for the request.
3. Select the domain from the **Available Domains** list.
4. Click the **Create certificate for the selected domain** checkbox to autofill the **Subject** field.
5. Select the Lifetime of the certificate. The lifetime can be 1, 2, or 3 years.
6. Click the Submit button.

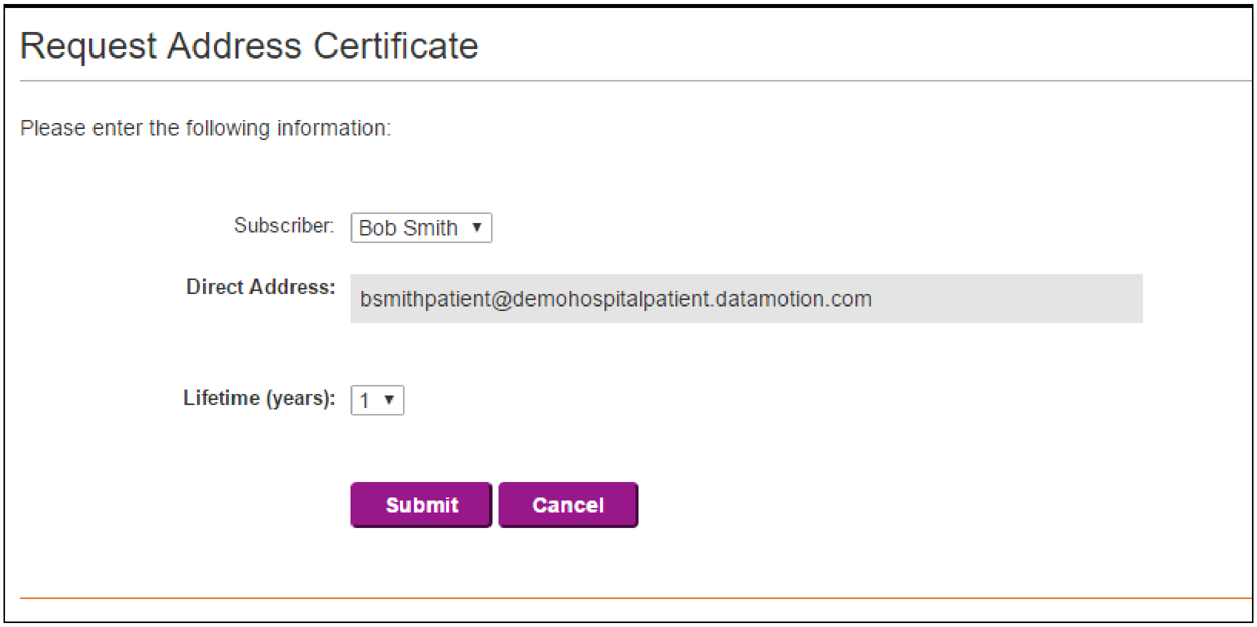
Every time a request is put in for an organizational certificate it is submitted for approval. A DataMotion Officer will handle and approve the request upon receiving the notification. The approved request is then submitted to the DataMotion CA/RA and properly generated. After this process is complete the certificate will be installed (the status of the installation can be checked on the Certificates Tab). Once installed, Direct Users may be provisioned who are to be covered by the certificate.

## ADDRESS CERTIFICATE REQUEST

Requesting an address certificate is performed in largely the same way as a requesting an organization certificate. A TA user and a validated domain are required in order to perform this task. It is worth noting that the recipients of address certs can only be validated ACS users.

1. On the Home page, click the **Certificates** tab, then the **Request Address Cert** link.
2. Select which user will receive the address certificate from the **Subscriber:** drop-down. Their Direct address will be populated automatically and cannot be edited.
3. Select the lifetime of the certificate using the **Lifetime (years):** drop-down. You can select either 1, 2, or 3 years.
4. Click the Submit button.

**Figure 25 – Request an Address Certificate**




The certificate will have to be approved by a DataMotion Officer at this time.

5. Upon approval the certificate will be installed completing the request cycle.

**NOTE: The selected user must be a validated ACS on the HCO, meaning they must have had their identity information as well as a Declaration of Identity Document submitted for approval by a DataMotion Officer.**

After a submission is approved, the ACS user will be provisioned onto the DMP with the Direct Address named on the cert. Following provisioning (which may take up to 45 minutes depending on load), the user will be able to send/receive Direct messages.

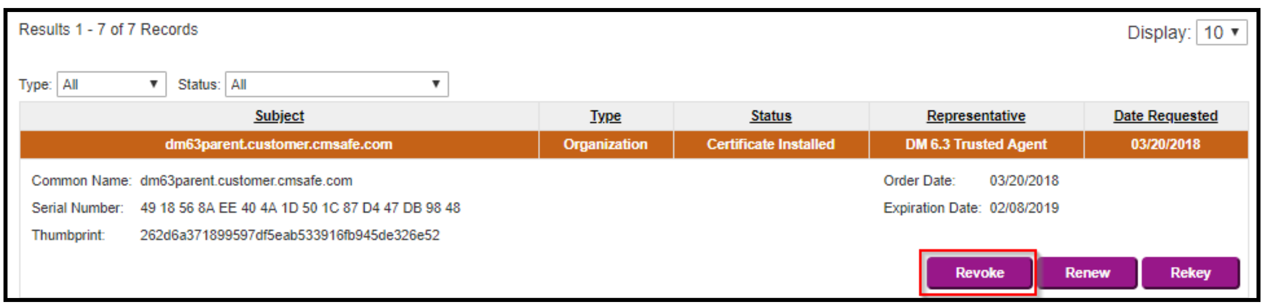
## REVOKING A CERTIFICATE

A DataMotion Officer is required to revoke active certificates unless Trusted Service is enabled (see *Validation and Enabling a Trusted Service*). Whenever a TA revokes a certificate within the HCO, a request to a DataMotion Officer will be submitted that cites the certificate to be revoked.

> **WARNING! Revoking an Organization certificate type will immediately terminate all account capabilities that are based on this certificate being valid. This includes account functions and Direct messaging send/receive capabilities for all users in the organization who are covered under the certificate, including TAs and Admins if they are covered by the same certificate.**

Perform the following steps to revoke a certificate.

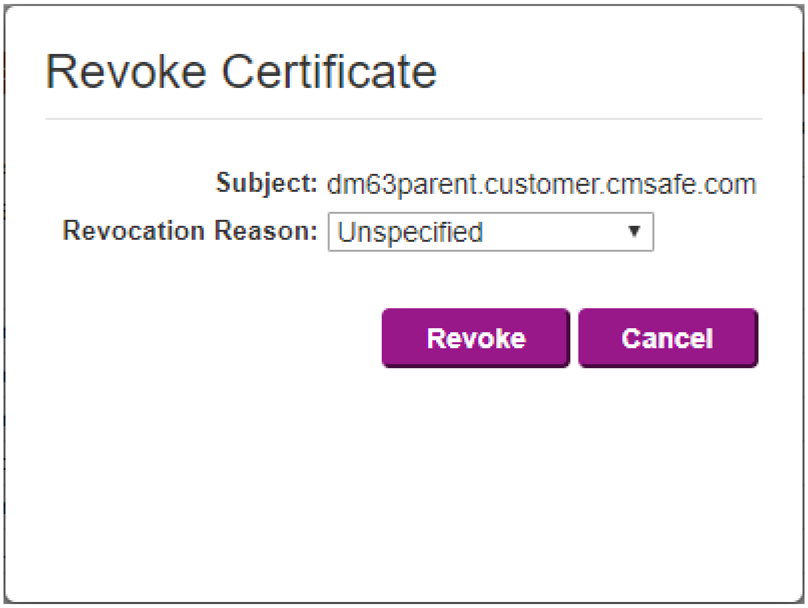
1. On the Home page click the Certificates tab.
2. Find the user whose certificate must be revoked and click it. Confirm that the Type field is **Address** (see preceding warning about revoking an Organization certificate, it is possible, but only recommended in the event of company deletion or domain change). Click the Revoke link to open the Revoke Certificate page.




3. Use the Revocation Reason drop-down to select the reason why this certificate is being revoked. Unspecified is the default option that appears, but in total there are 11 options which are listed below.
   - Unspecified
   - Key Compromise
   - Ca Compromise
   - Affiliation Changed
   - Superseded
   - Cessation of Operation
   - Certificate Hold
   - Obsolete 1
   - Remove From Crl
   - Privilege Withdrawn

» Aa Compromise

Figure 26 – Revoke Certificate




4. Click Revoke.

A DataMotion Officer will be notified and will approve the request. The TA will be notified by email or web that the certificate will be revoked and the certificate(s) will be removed from the HISP.

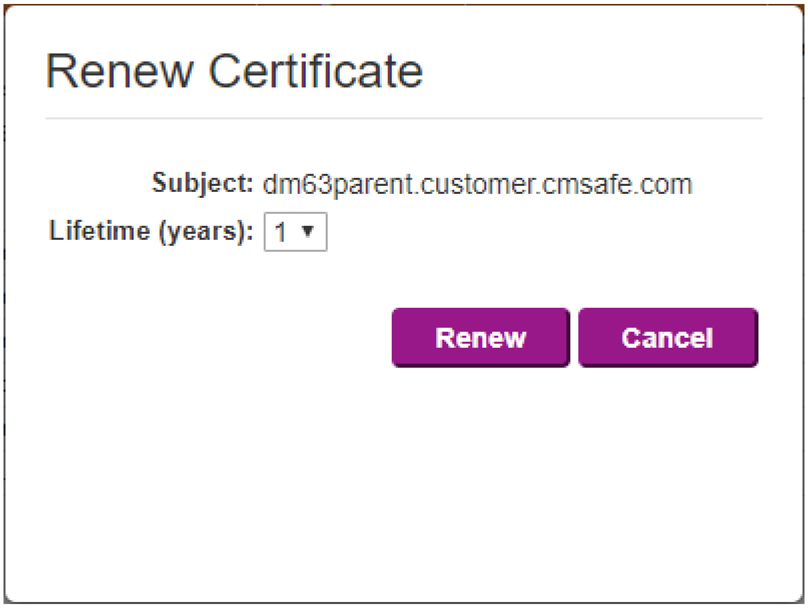
## RENEW A CERTIFICATE

When certificates are provisioned they will have a set number of years applied to them before they expire. If a certificate expires it will not be possible for it to be used anymore which will result in service disruption for any and all users covered by the certificate.

Perform the following steps to renew a certificate.

1. On the Home page click the Certificates tab.
2. Find the certificate you wish to renew and click it.
3. Click the Renew button.


4. Select the number of years in the pop-up.




5. Click Renew.

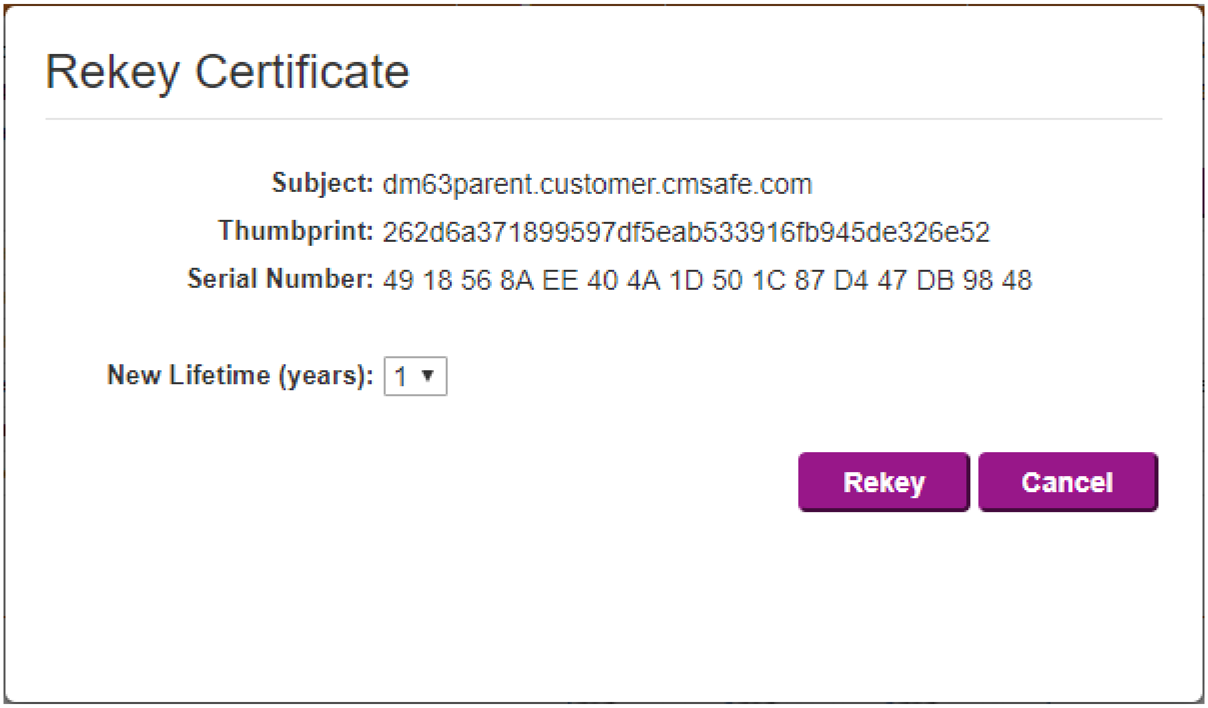
A DataMotion Officer will be notified and will approve the request. The TA will be notified by email or web that the certificate has been renewed.

### REKEY A CERTIFICATE

A certificate rekey is only necessary in the event of key compromise. Performing a rekey request will effectively return the same certificate just with a different key. There will be no increase in the expiration time of the certificate.

Perform the following steps to rekey a certificate.

1. On the Home page click the Certificates tab.
2. Find the certificate you wish to rekey and click it.
3. Click the Rekey button.




4. Click Rekey.

A DataMotion Officer will be notified and will approve the request. The TA will be notified by email or web that the certificate has been rekeyed.

## EDITING USERS

**NOTE: An Admin user can also perform the functionality described in this section with the exception of promoting an Admin user to a TA. That feature is limited to Trusted Agent's only.**

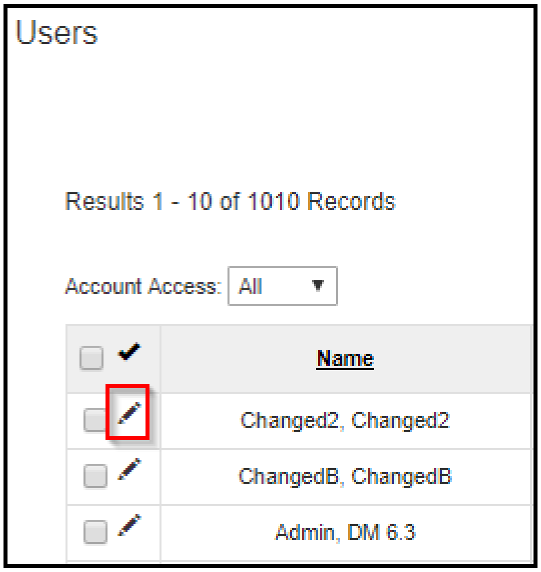
Over an organization's lifespan it is expected that users will have certain changes in their lives, such as their home address, phone number, email address, etc., so the option to edit users is available if a TA requires it. Editing a user should not be performed unless it is certain that the changes being made are accurate especially in the case of the Contact Email since that is where all notifications will be sent. Even more importantly, the Direct address of the user should not be altered unless it is absolutely certain that the user wishes for it to be changed. The Status of the user will be changed to **DmpUpdateRequired** until they sign in with their new address.

**NOTE: Appropriate notice should be given to any user that wants their Direct address to be changed (i.e. telling them their address has changed). They will NOT receive any notification from the DPP regarding the change, and attempts to sign in with the old address will fail.**

The editing functions serve a separate purpose by acting as a way to promote an Admin user to a Trusted Agent if desired by using the **Account Access** drop-down. Should this option be chosen, then all fields that are required for a TA user's creation will have to be satisfied.

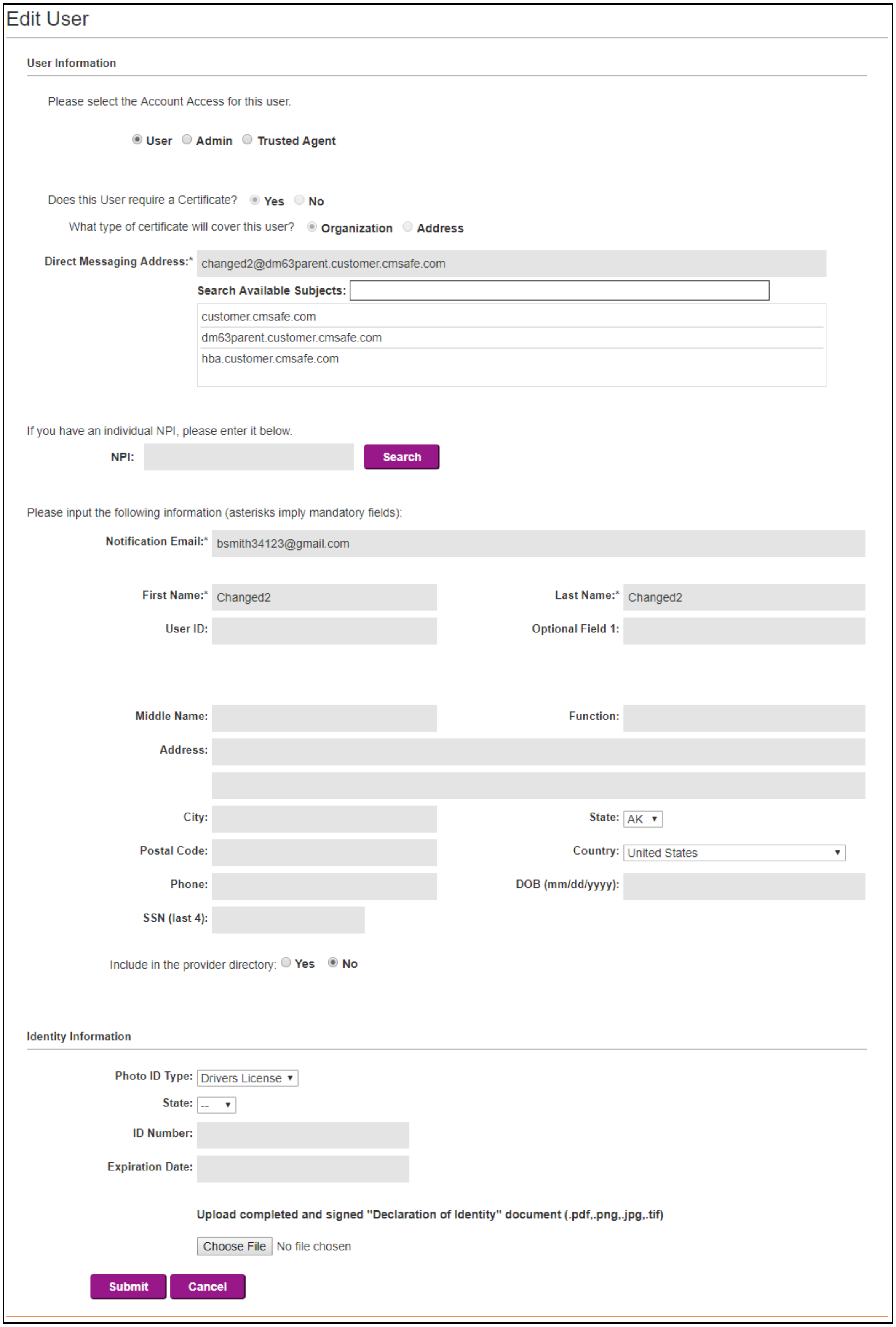
The Creating a New Trusted Agent section can provide details on what is necessary for a Trusted Agent as opposed to an Admin. To access the user editing page follow the steps described below.

1. On the Home page click the Users tab.
2. Click the edit text next to the user you want to edit.




3. The Edit User page will be displayed.

**Figure 27 – Edit User**




4. Any edits desired can be made using the fields on the page and then clicking Submit.

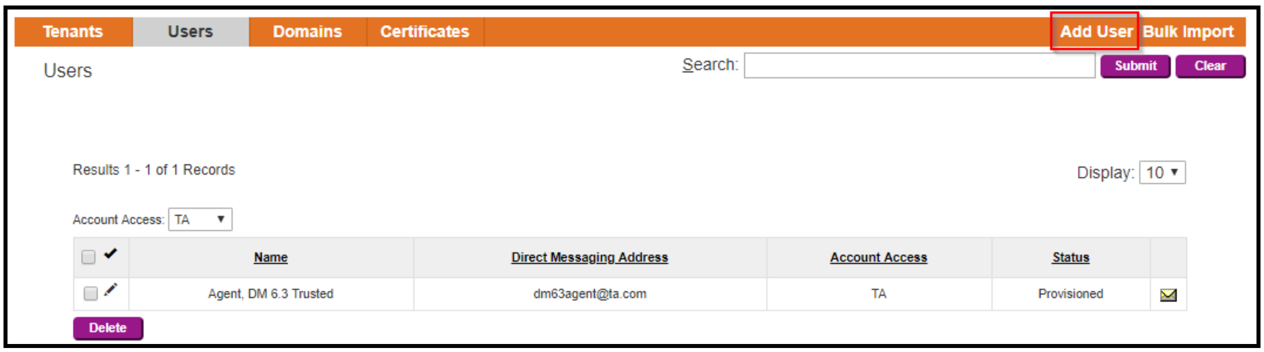
In some cases, additional actions will be required besides clicking the Submit button. These include upgrading an Admin user to a TA, and making any changes to an already existing TA user since validation will be required in both of these cases.

## CREATING A NEW TRUSTED AGENT

Every HCO that has a TA user is capable of creating additional TAs should it be necessary. The new TA users will have the same powers and capabilities as the existing TA, and can be assigned to administer any additional HCOs created at a lower level in the hierarchy. Creation of TAs is not limited to a specific number for any HCO, it is advised not to create more TAs than necessary.

The process to provision a TA user is relatively the same as it is during the third step of the Register Organization procedure. More specifically refer to the Step 3: Authorized User (Register Organization) section for more information.

1. On the Home page click the **Users** tab, and then click on **Add User**.




2. Select the TA radio button for the **Account Access** of the user and enter valid information for the following fields:

   **NOTE: If the NPI is entered it will auto-fill the page with the information contained in the user's NPI.**

   » Notification Types – Determines how the TA will receive their notifications, it is possible to select both checkboxes.

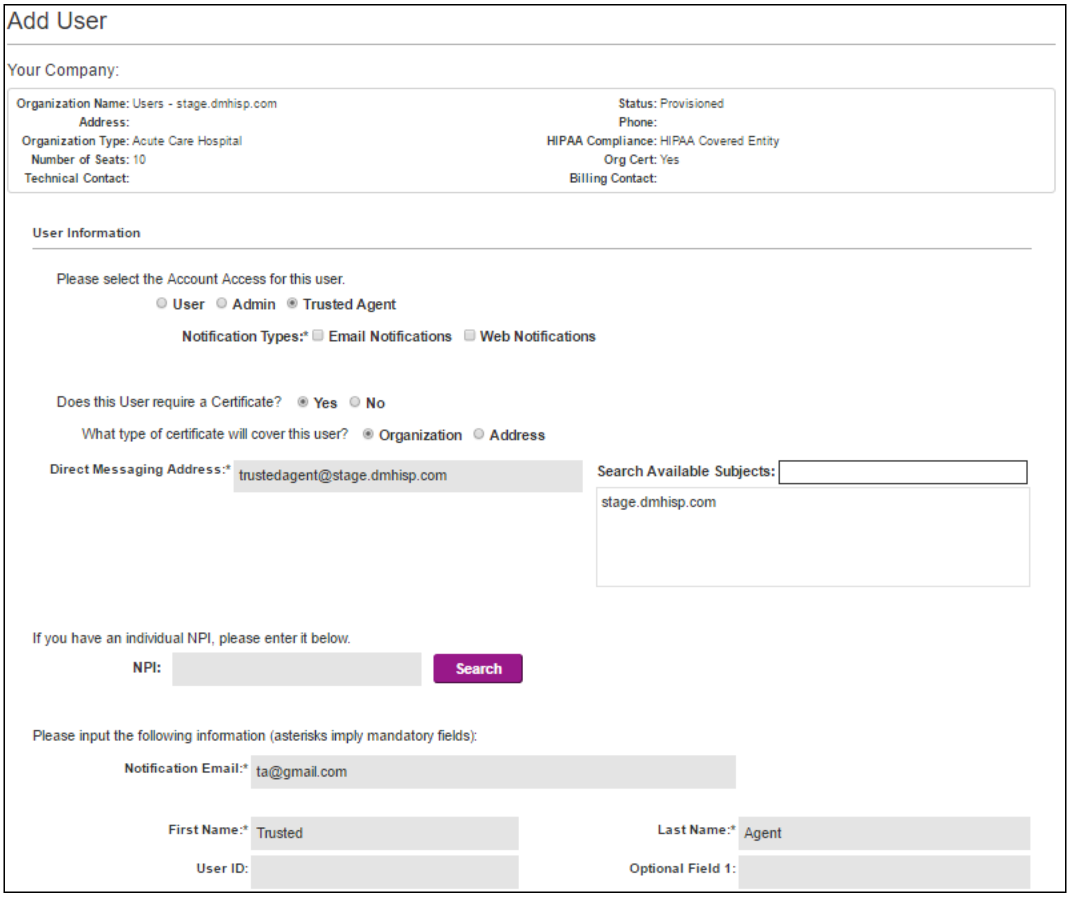
   » Certificate Required – The second set of radio buttons will ask if the Trusted Agent requires a certificate or not.

   » Certificate Type – The third set of radio buttons asks which certificate type will cover the user. Only Organization or Address may be selected, not both. This section will be grayed out if No is chose for the above step.

   » Direct Messaging Address – Enter the Direct Address for the Trusted Agent. When selecting the domain from the list on the right a "@" symbol and the domain will be placed in the text field. Depending on the Certificate Type chosen, these domains will be different (it is also possible for there to be no domains if none exist for the chosen Certificate Type).

- Notification Email – The notification email address is used to send notices about account and company activity (such as certificate installation) if the Email Notifications checkbox is selected.
- First Name – The first name of the TA.
- Last Name – The last name of the TA.

**Figure 28 – Create a new TA User for the organization Part A**


Add User

Your Company:

Organization Name: Users - stage.dmhisp.com
Address:
Organization Type: Acute Care Hospital
Number of Seats: 10
Technical Contact:
Status: Provisioned
Phone:
HIPAA Compliance: HIPAA Covered Entity
Org Cert: Yes
Billing Contact:

User Information

Please select the Account Access for this user.
User Admin Trusted Agent
Notification Types:* Email Notifications Web Notifications

Does this User require a Certificate? Yes No
What type of certificate will cover this user? Organization Address
Direct Messaging Address:* trustedagent@stage.dmhisp.com
Search Available Subjects:
stage.dmhisp.com

If you have an individual NPI, please enter it below.
NPI: Search

Please input the following information (asterisks imply mandatory fields):
Notification Email:* ta@gmail.com
First Name:* Trusted
Last Name:* Agent
User ID:
Optional Field 1:

- Address – The home address of the Trusted Agent.
- City – The city/town of the TA's address.
- State – The state which the city is located.
- Postal Code – 5 digit postal code for the TA's address.
- Country – The country where the TA resides.
- Include in the provider directory – If yes the user will be included in the HPD (only shown if the company has the "Include this HCO and its users in the Healthcare Provider Directory" enabled, see the *Editing an HCO* section for details).
- Photo ID Type – Use the drop-down to select which type of photo identity is being submitted. The options available are either Driver's License, State ID, or Passport.

**NOTE: If Driver's License or State ID is selected, the State drop-down will be required. If Passport is selected then the State drop-down will not appear.**

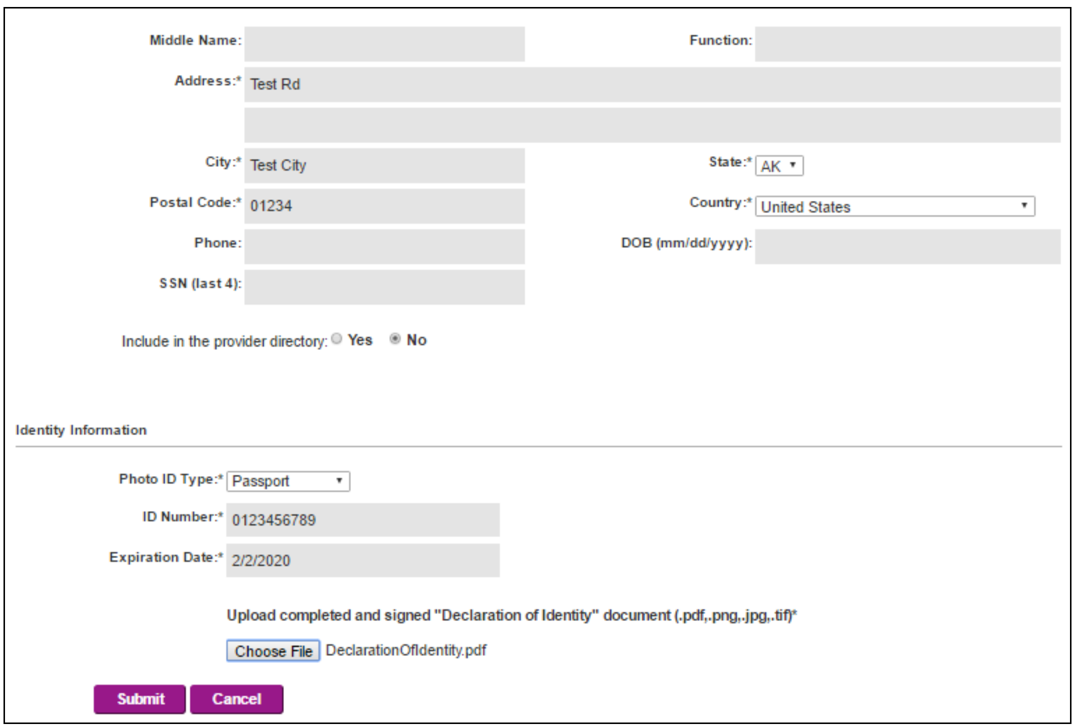
- State (if applicable) – Use the drop-down to select the state that the photo identity was issued in.

**NOTE: Depending on the State selected for the Photo ID it may be necessary to submit a second Photo ID. See the Prerequisites section and more specifically the** *NOTE Regarding Photo ID Submission on page 32* **if it is not possible to satisfy the requirements of the second Photo ID.**

- ID Number – Enter the serial number for the selected identity type. In the case of a driver's license this is usually the number next to either DL, ID, Number, or NO.
- Expiration Date – The expiration date of the Photo ID being submitted.
- Declaration of Identity Document: A completed DoID must be uploaded. The DoID must either be filled out/signed in the presence of an already validated TA, or a Notary public. If you need to download a blank DoID, be sure to open the ***Support*** screen (see page 30) in a new browser tab to avoid exiting the application process.

**NOTE: The information entered into the DoID should match the information entered throughout these instructions.**

**Figure 29 – Creating a new TA User for the organization Part B**




3. Select Submit to send the information to the Registration Authority, RA, for approval.
   - The new TA will receive an email notification with instructions for creating a DPP account. See ***Establish Your Account*** (on page 17).

This completes the process to create another TA for an HCO.

# 5
# Administrative Actions

**NOTE: All actions that can be performed by an administrator can also be performed by a Trusted Agent. An Admin user can also perform the** *Editing Users* **functions** *on page 54* **with the exception of promoting users to the TA user type.**

## USER PROVISIONING

Once your HCO has the certificates that it requires, you will be able to provision users to the portal. Provisioning users can be performed either individually via entering information into the appropriate fields, or in groups by selecting the **Bulk Upload** option. In addition to being able to create a Direct user, it is possible to create additional Administrators. Additional Trusted Agents can also be created but only by other Trusted Agents (see the *Creating a New Trusted Agent* section *on page 57*.

### ADDING A SINGLE DIRECT USER

Your HCO can provision a Direct user if they have an authorized TA within their company or one is assigned to them via the parent HCO. If the user you are attempting to add is going to be covered under an organization certificate, they will be immediately activated and added upon successful submission. Should the user you are attempting to add be covered under an address certificate, the submission will require manual approval by a DataMotion Officer for the user to be added.

All information that is pertinent to the user being added should be gathered before attempting to add them to speed up the process. Please note that there are some conditions that apply to adding Direct Users. These are as follows:

- A user that is to be covered by an address certificate under the domain of an organization certificate is not allowed.
- All users to be added to the portal must have Direct addresses, i.e. they cannot be regular email addresses or it will be impossible to add them to the HCO.

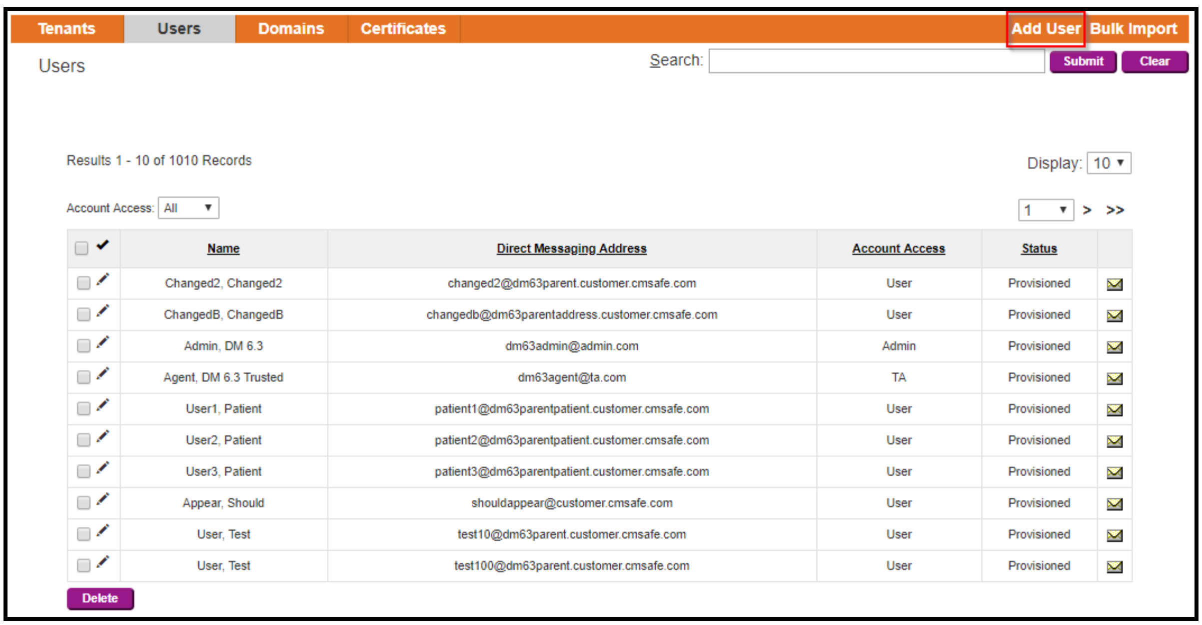
- No Direct address can be duplicated. As a result, it is impossible to add a Direct user where there is a Direct address conflict that would result in the HCO having two of the same Direct address.
- You can send the notifications of multiple Direct users to the same email notification address if necessary.

Taking these factors into account you should be ready to add Direct users to an organization. Perform the following steps to add a Direct user to the HCO of your choosing.

## Adding a Direct User covered by an Address Certificate

A Direct user covered by an Address certificate is also known as an Address Certificate Subscriber. The process to add a user of this type is almost identical to the process to add a new Trusted Agent described in the *Creating a New Trusted Agent* section. To add a Direct User covered by an Address Certificate follow the steps below.

1. On the Home page click the **Users** tab, and then click on **Add User**.




2. Select the User radio button for the **Account Access** of the user and enter valid information for the following fields:

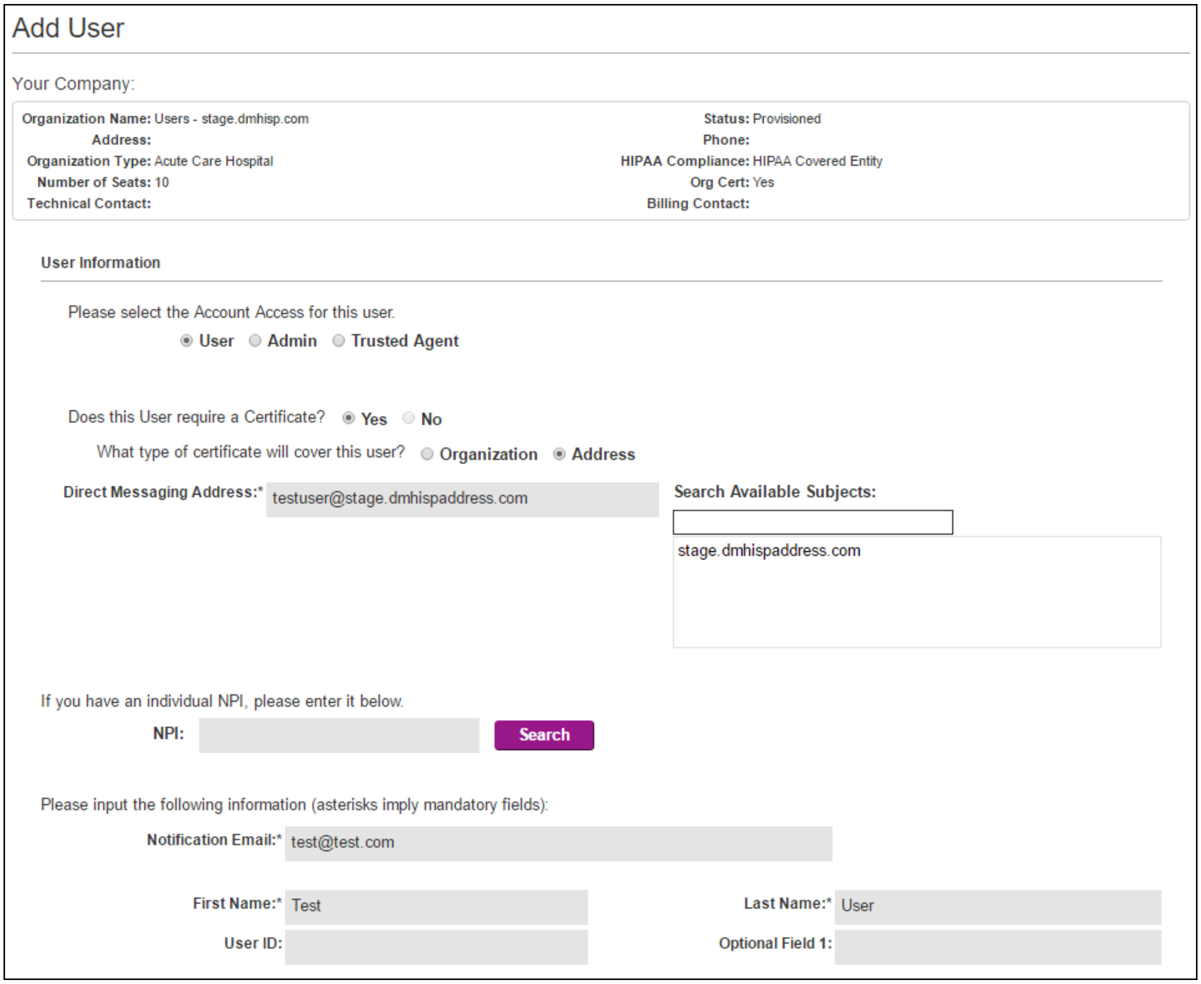
**NOTE: If the NPI is entered it will auto-fill the page with the information contained in the user's NPI.**

» Certificate Type – The second set of radio buttons asks which certificate type will cover the user. Only Organization or Address may be selected, not both, but for these instructions select Address.

» Direct Messaging Address – Enter the Direct Address for the Direct User. When selecting the domain from the list on the right a "@" symbol and the domain will be placed in the text field. Depending on the Certificate Type chosen, these domains will be different (it is also possible for there to be no domains if none exist for the chosen Certificate Type).

- Notification Email – The notification email address is used to send notices about account and company activity to the user for account creation and password info.
- First Name – The first name of the Direct User.
- Last Name – The last name of the Direct User.

**Figure 30 – Adding an Address Certificate Subscriber (ACS) Direct User Part A**




- Address – The home address of the Direct User.
- City – The city/town of the Direct User's address.
- State – The state which the city is located.
- Postal Code – 5 digit postal code for the Direct User's address.
- Country – The country where the Direct User resides.

- » Include in the provider directory – If yes, the user will be included in the HPD (only shown if the company has the "Include this HCO and its users in the Healthcare Provider Directory" enabled, see the *Editing an HCO* section for details).
- » Photo ID Type – Use the drop-down to select which type of photo identity is being submitted. The options available are either Driver's License, State ID, or Passport.

**NOTE: If Driver's License or State ID is selected, the State drop-down will be required. If Passport is selected then the State drop-down will not appear.**

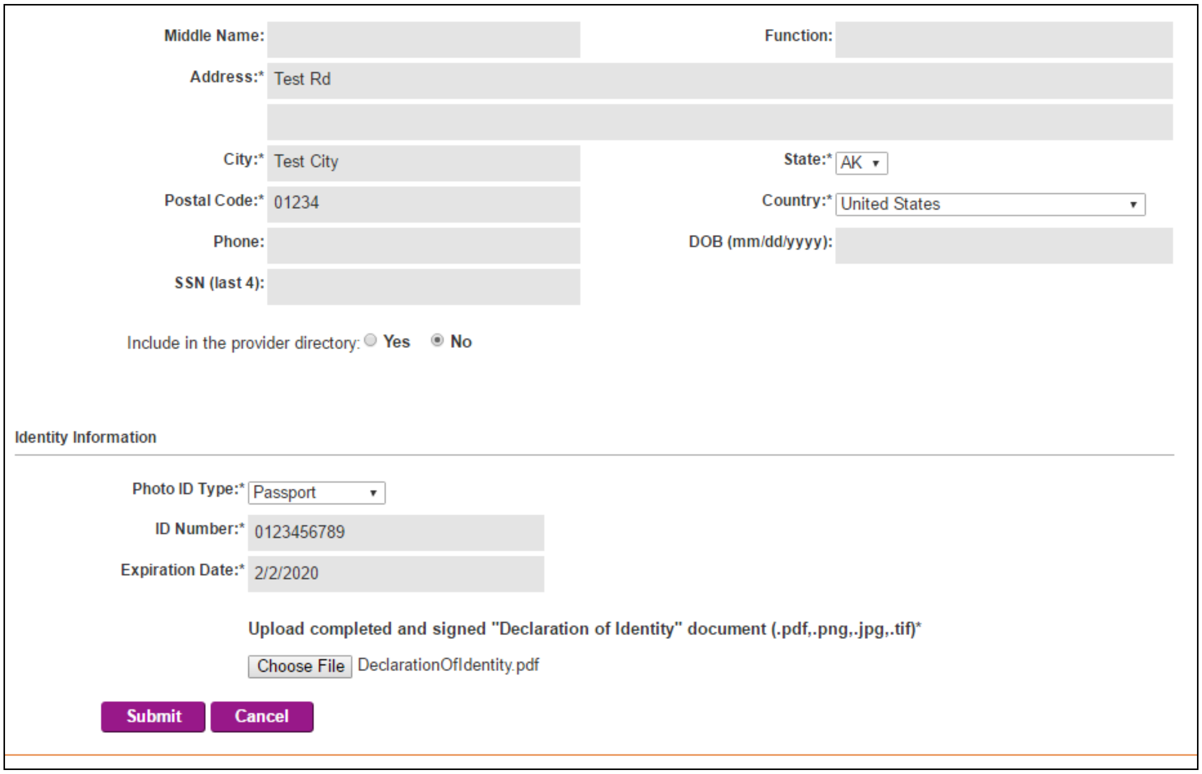
- » State (if applicable) – Use the drop-down to select the state that the photo identity was issued in.

**NOTE: Depending on the State selected for the Photo ID it may be necessary to submit a second Photo ID. See the section and more specifically the** *NOTE Regarding Photo ID Submission on page 32* **if it is not possible to satisfy the requirements of the second Photo ID.**

- » ID Number – Enter the serial number for the selected identity type. In the case of a driver's license this is usually the number next to either DL, ID, Number, or NO.
- » Expiration Date – The expiration date of the Photo ID being submitted.
- » Declaration of Identity Document: A completed DoID must be uploaded. The DoID must either be filled out/signed in the presence of an already validated TA, or a Notary public. If you need to download a blank DoID, be sure to open the *Support* screen (see page 30) in a new browser tab to avoid exiting the application process.

**NOTE: The information entered into the DoID should match the information entered throughout these instructions.**

**Figure 31 – Adding an Address Certificate Subscriber (ACS) Direct User Part B**




3. Select Submit to send the information to the Registration Authority, RA, for approval.
   » The new TA will receive an email notification with instructions for creating a DPP account. See *Establish Your Account* (on page 17).

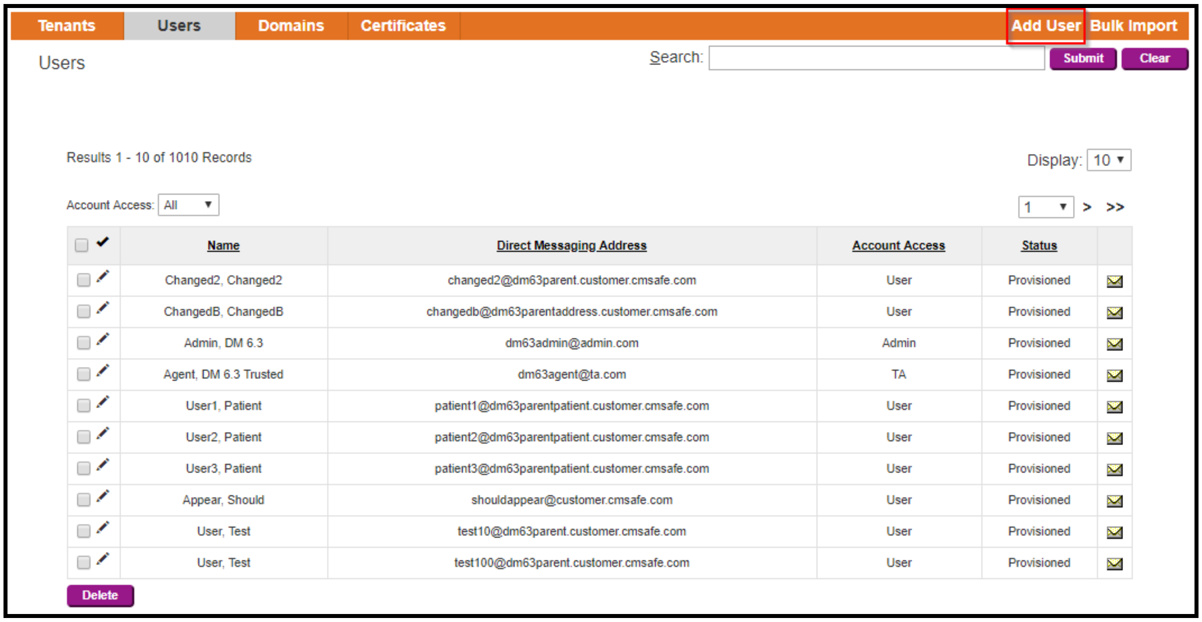
This completes the process for adding a Direct User covered by an Address Certificate to an HCO.

**NOTE: While the user may have been added to the DPP upon completion of this process, a certificate will have to be requested in order for them to be successfully validated and provisioned to use Direct Messaging. This requires a Trusted Agent to perform the *Address Certificate Request* process and wait for certificate approval by a DataMotion Officer.**

## Adding a Direct User covered by an Organization Certificate

A Direct user covered by an Organization Certificate does not need to undergo approval in the same way that the Address Certificate Subscriber does. The Organization Certificate itself signifies that all users added under the domain are authorized to use Direct Messaging related services. To add a Direct User covered by an Organization Certificate follow the steps below.

1. On the Home page click the **Users** tab, and then click on **Add User**.




| | Name | Direct Messaging Address | Account Access | Status |
|---|---|---|---|---|
| | Changed2, Changed2 | changed2@dm63parent.customer.cmsafe.com | User | Provisioned |
| | ChangedB, ChangedB | changedb@dm63parentaddress.customer.cmsafe.com | User | Provisioned |
| | Admin, DM 6.3 | dm63admin@admin.com | Admin | Provisioned |
| | Agent, DM 6.3 Trusted | dm63agent@ta.com | TA | Provisioned |
| | User1, Patient | patient1@dm63parentpatient.customer.cmsafe.com | User | Provisioned |
| | User2, Patient | patient2@dm63parentpatient.customer.cmsafe.com | User | Provisioned |
| | User3, Patient | patient3@dm63parentpatient.customer.cmsafe.com | User | Provisioned |
| | Appear, Should | shouldappear@customer.cmsafe.com | User | Provisioned |
| | User, Test | test10@dm63parent.customer.cmsafe.com | User | Provisioned |
| | User, Test | test100@dm63parent.customer.cmsafe.com | User | Provisioned |

2. Select the User radio button for the **Account Access** of the user and enter valid information for the following fields:

**NOTE: If the NPI is entered it will auto-fill the page with the information contained in the user's NPI.**

- Certificate Type – The second set of radio buttons asks which certificate type will cover the user. Only Organization or Address may be selected, not both, but for these instructions select Organization.
- Direct Messaging Address – Enter the Direct Address for the Direct User. When selecting the domain from the list on the right a "@" symbol and the domain will be placed in the text field. Depending on the Certificate Type chosen, these domains will be different (it is also possible for there to be no domains if none exist for the chosen Certificate Type).
- First Name – The first name of the Direct User.
- Last Name – The last name of the Direct User.

**Figure 32 – Adding a Direct User covered under an Organization Certificate Part A**

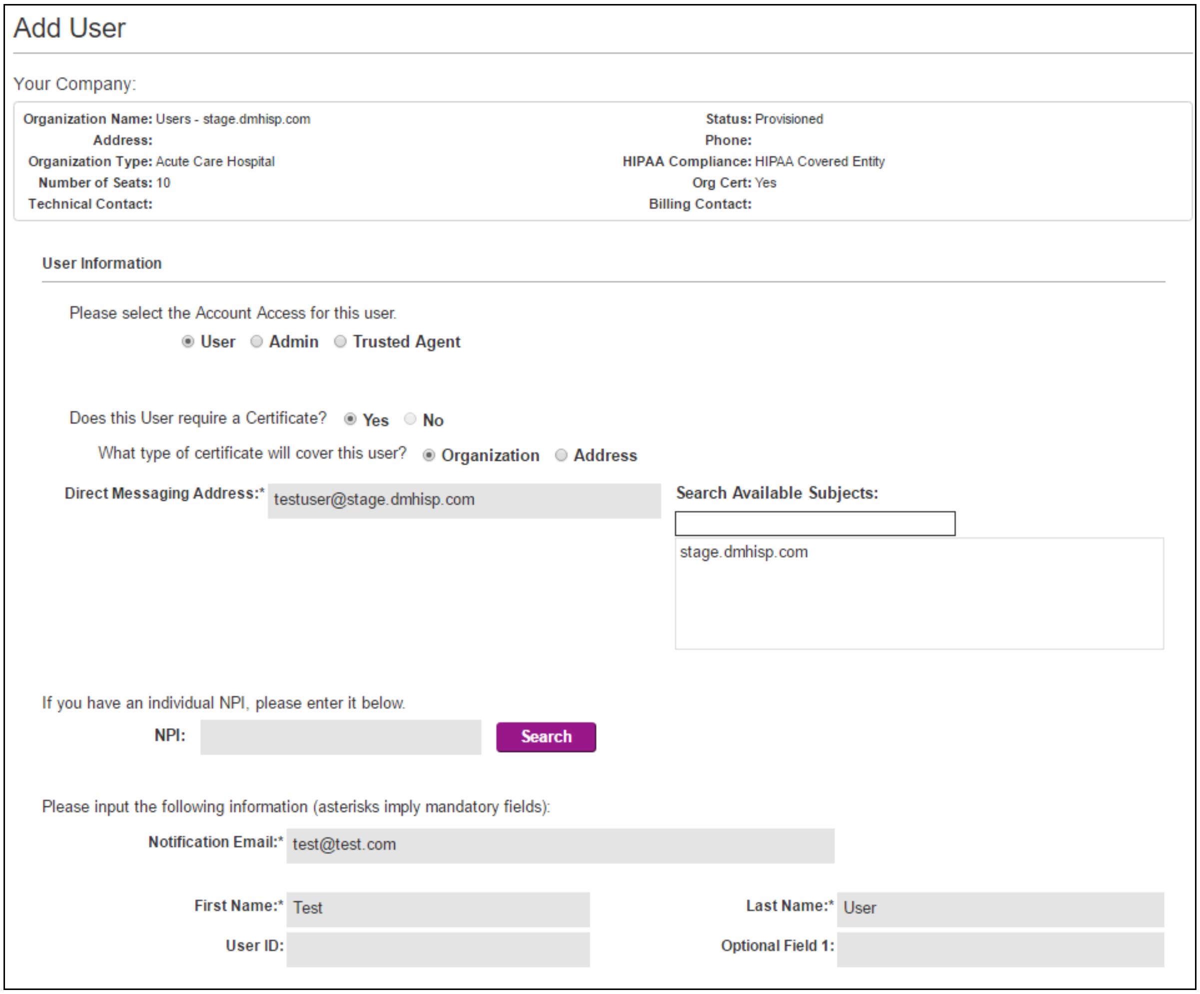
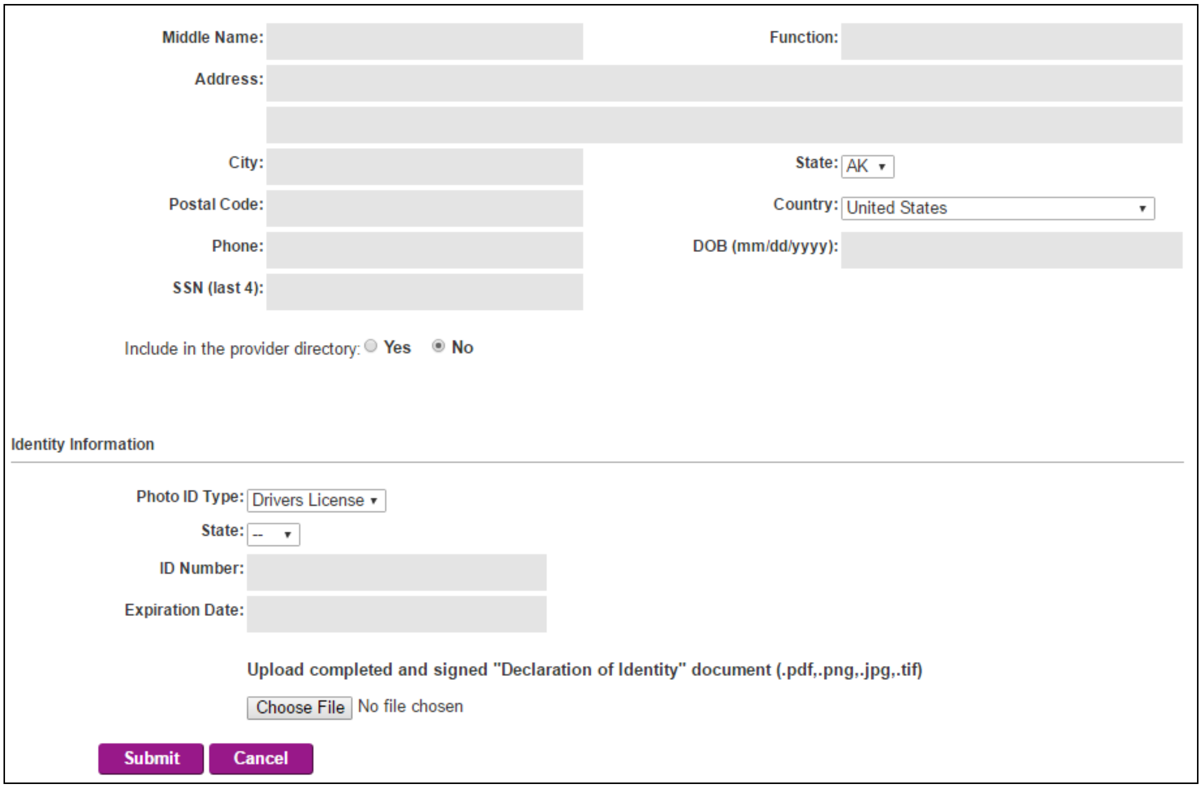


**Figure 33 – Adding a Direct User covered under an Organization Certificate Part B**



Middle Name: | Function:
Address:
City: | State: AK
Postal Code: | Country: United States
Phone: | DOB (mm/dd/yyyy):
SSN (last 4):

Include in the provider directory: Yes No

Identity Information

Photo ID Type: Drivers License
State: --
ID Number:
Expiration Date:

Upload completed and signed "Declaration of Identity" document (.pdf,.png,.jpg,.tif)

Choose File No file chosen

Submit Cancel

» Include in the provider directory – If yes, the user will be included in the HPD (only shown if the company has the “Include this HCO and its users in the Healthcare Provider Directory” enabled, see the *Editing an HCO* section for details).

3. Select Submit.

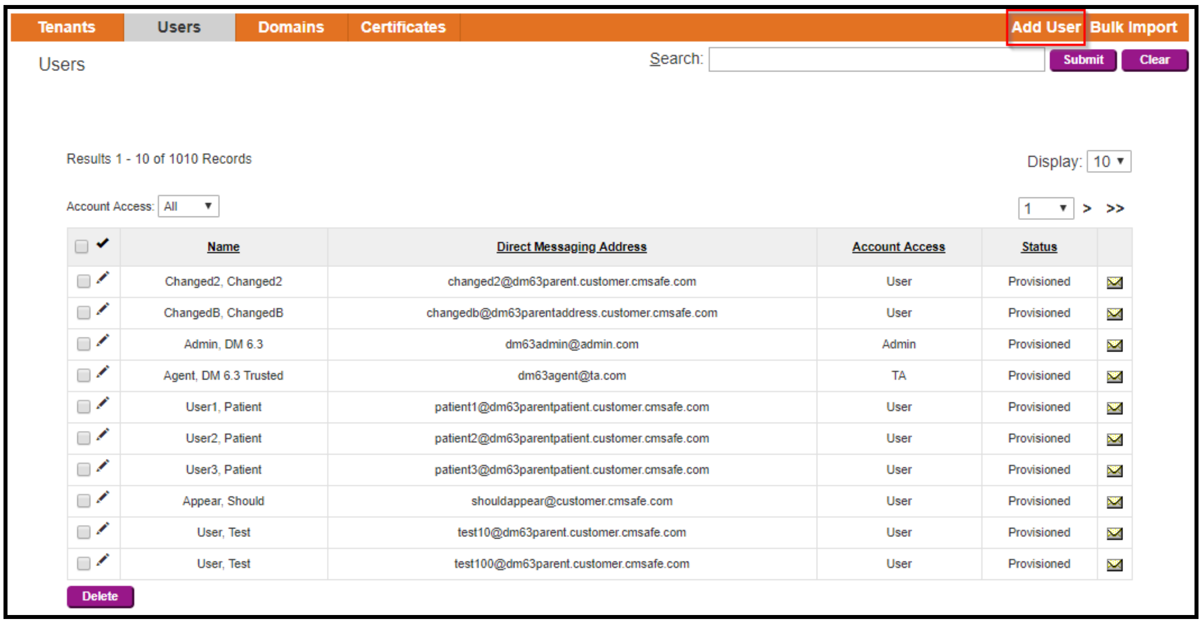
This completes the process for adding a Direct User covered by an Organization Certificate to an HCO.

**NOTE: The user will be automatically provisioned upon completion.**

## ADDING AN ADMINISTRATIVE USER

All HCO's have the capability to create Admin users at will without the need for any identity validation. The certificate type chosen for the Admin does not change this fact. A Direct address is required for the Admin user and a seat will be consumed for this user. To add an Admin user follow the steps below.

1. On the Home page click the **Users** tab, and then click on **Add User**.




| | Name | Direct Messaging Address | Account Access | Status |
|---|---|---|---|---|
| | Changed2, Changed2 | changed2@dm63parent.customer.cmsafe.com | User | Provisioned |
| | ChangedB, ChangedB | changedb@dm63parentaddress.customer.cmsafe.com | User | Provisioned |
| | Admin, DM 6.3 | dm63admin@admin.com | Admin | Provisioned |
| | Agent, DM 6.3 Trusted | dm63agent@ta.com | TA | Provisioned |
| | User1, Patient | patient1@dm63parentpatient.customer.cmsafe.com | User | Provisioned |
| | User2, Patient | patient2@dm63parentpatient.customer.cmsafe.com | User | Provisioned |
| | User3, Patient | patient3@dm63parentpatient.customer.cmsafe.com | User | Provisioned |
| | Appear, Should | shouldappear@customer.cmsafe.com | User | Provisioned |
| | User, Test | test10@dm63parent.customer.cmsafe.com | User | Provisioned |
| | User, Test | test100@dm63parent.customer.cmsafe.com | User | Provisioned |

Delete

2. Select the Admin radio button for the **Account Access** of the user and enter valid information for the following fields:

**NOTE: If the NPI is entered it will auto-fill the page with the information contained in the user's NPI.**

» Notification Types – Determines how the Admin will receive their notifications, it is possible to select both checkboxes.

» Certificate Required – The second set of radio buttons will ask if the Trusted Agent requires a certificate or not.

» Certificate Type – The third set of radio buttons asks which certificate type will cover the user. Only Organization or Address may be selected, not both. This section will be grayed out if No is chose for the above step.

» Direct Messaging Address – Enter the Direct Address for the Admin. The drop-down to the right of the "@" symbol must be used to select the domain. Depending on the Certificate Type chosen, these domains will be different (it is also possible for there to be no domains if none exist for the chosen Certificate Type).

» First Name – The first name of the Admin.

» Last Name – The last name of the Admin.

**Figure 34 – Adding an Admin User Part A**

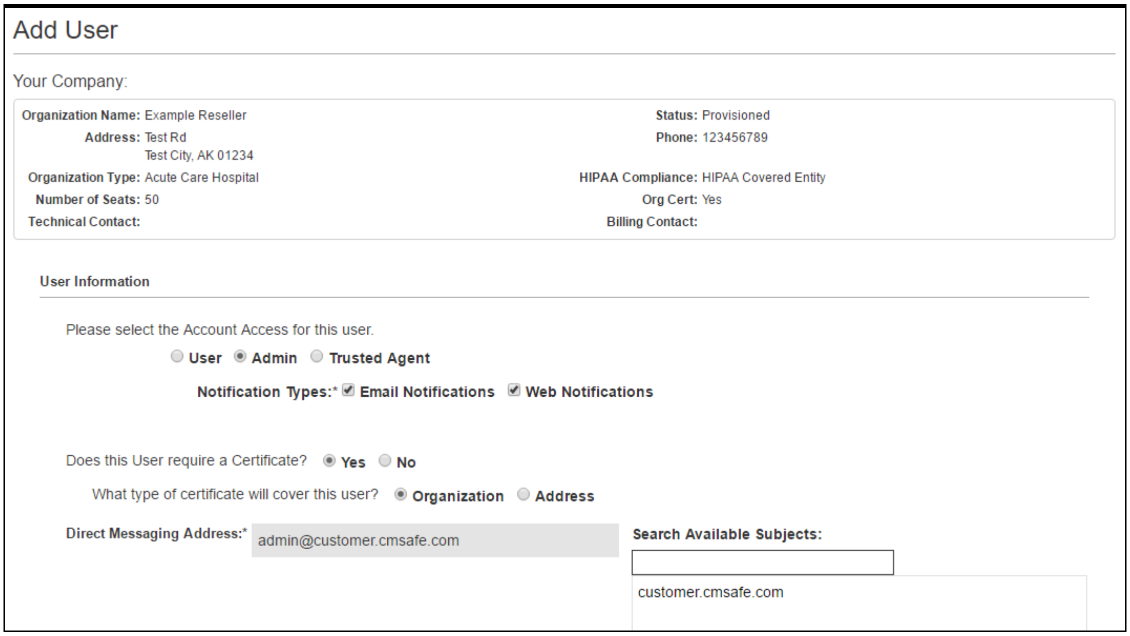
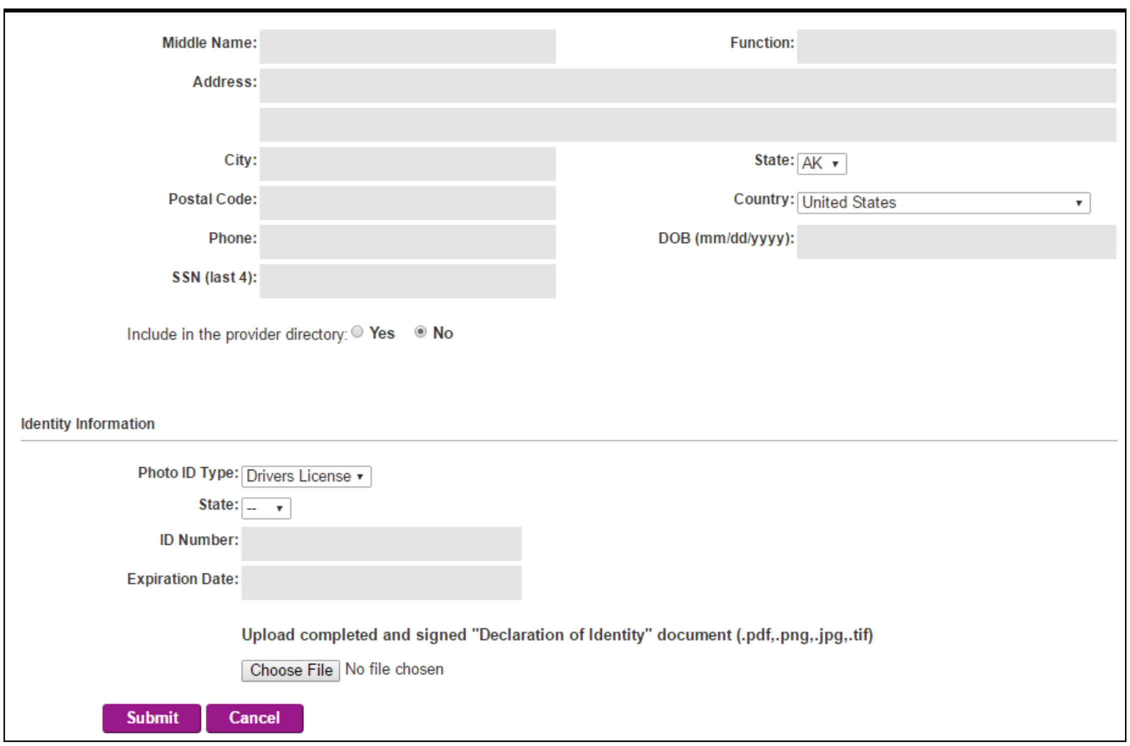



**Figure 35 – Adding an Admin User Part B**




» Include in the provider directory – If yes, the user will be included in the HPD (only shown if the company has the "Include this HCO and its users in the Healthcare Provider Directory" enabled, see the *Editing an HCO* section for details).

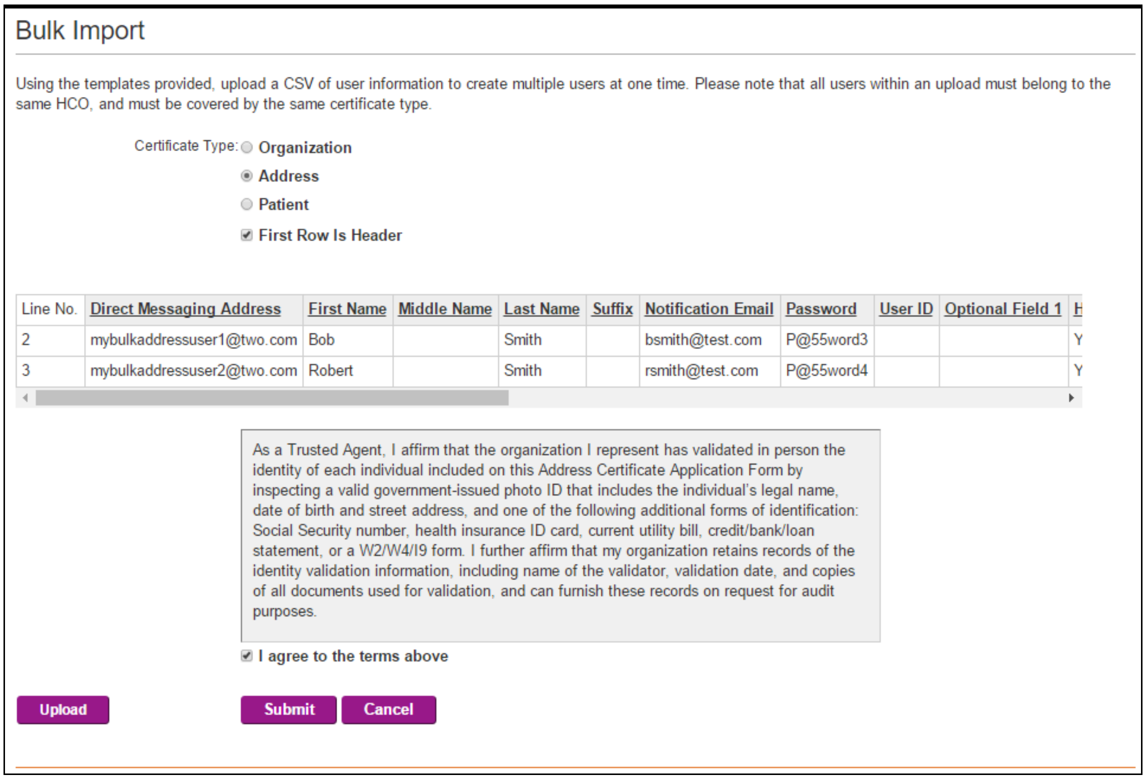
3. Select Submit.

The user will be sent a notification email telling them to create their account as described in the Creating Your Login Credentials section.

## PROVISIONING MULTIPLE DIRECT USERS VIA BULK IMPORT

By using Bulk Import, it is possible for a TA to add a CSV of users into the portal. The Bulk Import can be used for users that will be covered by an organization certificate, address certificates, or patient certificates.

**Figure 36 – Submitting a CSV via Bulk Import**




Refer to the Bulk Import sections to determine the format of the CSV that you must use and follow the steps below to submit the Bulk Upload.

1. On the Home page, click the Users tab and select Bulk Import.
2. Select the Certificate Type that you will be using to add the users.
   » You can download a template for the CSV to upload by navigating to the Support page. See *Figure 12 – Support Requests and Documentation* for more information.

**NOTE: The downloaded templates are in .xlsx format which is unique to Microsoft Excel. However, if you do not have Microsoft Excel you can use a free alternative such as Google Docs to fill out the spreadsheet. When finished please ensure that you save the spreadsheet as .CSV or it will not be possible to submit it.**

**NOTE: If you select Address or Patient as the** Certificate Type**, a gray window will appear containing terms of service which is the same as displayed in the sample image on page 71. This terms of service must be accepted via a check box that states** I agree to the terms above**.**

3. Click the **Upload** button to access an open file dialog box and select the CSV that you want to upload.

**NOTE: If you used a template located on the Support page and retained the first row of the spreadsheet, select the First Row is Header checkbox in order to signify this.**

4. Click the **Submit** button.

## Bulk Import for users covered under an organization certificate

**NOTE: An Organization Certificate must already be in place for the domains being used by the Direct Users being uploaded. If not, the submission will fail.**

Using bulk upload for users covered under an organization certificate is a simple but effective way to add more than a single user at a time to the web portal. Ensure that the Admin user has gathered the appropriate information that is required for every user to be added and generate a CSV before attempting the upload. The upload will not succeed if any of the user information contained within the CSV is missing or invalid.

In order to ensure that the CSV entered by the Admin user is valid upon upload, refer to the table below to properly structure the CSV.

**Table 3 – CSV structure for bulk upload (Organization Certificate)**

| Field | Description | Required Field? | Output example |
|---|---|---|---|
| Direct Messaging Address | The Direct address of the user being added | Yes | jsmith@direct.test.com |
| First Name | The user's first name | Yes | John |
| Middle Name | The user's middle name | No | Parker |
| Last Name | The user's last name | Yes | Smith |
| Suffix | The suffix of the user | No | Jr |
| Notification Email | Email address where the user shall receive all of their notifications | Yes | jpi@gmail.com |

| | | | |
|---|---|---|---|
| Password | The password of the user being added. This prevents account registration notifications from being sent. | No | P@55word |
| User ID | The ID of the user to be displayed on the Direct Messaging Portal | No | Test User |
| Optional Field 1 | This field does not provide information | No | |
| Healthcare Provider? | Is the User a healthcare provider? | Yes | Can be Yes or No **(Must be entered as Y or N)** |
| HPD Authorization | This user will be published in the DataMotion Healthcare Provider Directory unless noted otherwise | Yes | By default the answer is yes. You can change the answer to No by writing **Do Not Publish** in this field. |
| Inherit Org Hpd Info | The user will inherit the organizational info of the company itself and will display the information in the HPD. | Yes | N (This is the default, can be changed to Yes by entering Y) |
| Hpd Organization Name | The organization name of the user to display in the HPD. This field should be left blank if the Inherit Org Hpd Info is set to Y | Yes | Company |
| User NPI | The NPI of the user (if applicable) only | No (if the NPI is known/available it is advised that it be entered for | 2222222222 |

| | | | |
|---|---|---|---|
| | | convenience in the future) | |
| User Specialty | The Specialty of the user | No (however if the NPI is not entered, then this field does become a required field) | Cardiology (or leave blank if NPI is entered) |
| User Role | The role of the user within the organization | Yes | Doctor |
| Address (Line 1) | The Address line 1 of the practice location | Yes | 1 Town Rd (if the NPI is entered this field will be pulled from there) |
| Address (Line 2) | The Address line 2 of the practice location | Yes | Suite 405 (if the NPI is entered this field will be pulled from there) |
| City | The city of the practice location | Yes | NewCity (if the NPI is entered this field will be pulled from there) |
| State Province Code | The state of the practice location | Yes | AK (If the NPI is entered this field will be pulled from there) |
| Postal Code | The postal code of the practice location | Yes | 01234 (if the NPI is entered this field will be pulled from there) |
| Phone | The phone number of the practice | Yes | 123-456-7890 (if the NPI is entered this field will be pulled from there) |
| Fax | The fax number of the practice | No | 098-765-4321 (if the NPI is entered this field will be pulled from there) |

Once every user in the CSV has all of these fields satisfied, the Admin can select Upload which will prompt a file dialog where they can select the CSV. After selection they can select the **Submit** button to submit the CSV (since these users are covered by an Organization Certificate they will be provisioned automatically). See *Figure 36 – Submitting a CSV* and the instructions that coincide with it on page 71 for information regarding the submission process.

All added users shall be notified of their accounts via an email notification that is sent to their Notification Email specified in the CSV (unless the Password field was specified). Once the users have been provisioned they shall be able to send and receive Direct messages.

## Bulk Import for users covered under address certificates

Users that are covered by address certificates can also be added via Bulk Upload. Ensure that the Admin user has gathered the appropriate information that is required for every user to be added and generate a CSV before attempting the upload. The upload will not succeed if any of the user information contained within the CSV is missing or invalid.

In order to ensure that the CSV entered is valid upon upload, refer to the table below to properly structure the CSV. Note that two types of valid identity documents must be stated in the CSV since address certificates are being used. The actual documents themselves are not required in the CSV itself. Simply stating what type of document (i.e. Driver's License) will suffice.

**Table 4 – CSV structure for bulk upload (Address Certificate)**

| Field | Description | Required Field? | Output Example |
|---|---|---|---|
| Direct Messaging Address | The Direct Address of the user | Yes | henry.smith@direct.mytowndocs.com |
| First Name | The user's first name | Yes | Henry |
| Middle Name | The user's middle name | No | |
| Last Name | The user's last name | Yes | Smith |
| Suffix | The suffix of the user | No | III |
| Notification Email | Email address where the user shall receive all their notifications | Yes | hs@gmail.com |
| Password | The password of the user being added. This prevents account registration notifications from being sent. | No | P@55word |
| User ID | The ID of the user to be displayed on the Direct Messaging Portal | No | Test User |

| | | | |
|---|---|---|---|
| Optional Field 1 | This field does not provide information | No | |
| Healthcare Provider? | Is the User a healthcare provider? | Yes | Can be Yes or No **(Must be entered as Y or N)** |
| HPD Authorization | This user will be published in the DataMotion Healthcare Provider Directory unless noted otherwise | Yes | By default the answer is yes. You can change the answer to no by writing **Do Not Publish** in this field. |
| Inherit Org Hpd Info | The user will inherit the organizational info of the company itself and will display the information in the HPD. | Yes | N (This is the default, can be changed to Yes by entering Y) |
| Hpd Organization Name | The organization name of the user to display in the HPD. This field should be left blank if the Inherit Org Hpd Info is set to Y | Yes | Company |
| User NPI | The NPI of the user (if applicable) only | No (if the NPI is known/available it is advised that it be entered for convenience in the future) | 3333333333 |
| User Specialty | The Specialty of the user | No (however if the NPI is not entered, then this field does become a required field) | Neurology (or leave blank if NPI is entered) |
| User Role | The role of the user within the organization | Yes | Surgeon |
| Address | The Address line 1 of the practice | Yes | 1 Town Rd (if the NPI is entered this field will be pulled from there) |

| | | | |
|---|---|---|---|
| | location | | |
| Address2 | The Address line 2 of the practice location | Yes | Suite 204 (if the NPI is entered this field will be pulled from there) |
| City | The city of the practice location | Yes | NewCity (if the NPI is entered this field will be pulled from there) |
| State Province Code | The state of the practice location | Yes | AK (If the NPI is entered this field will be pulled from there) |
| Postal Code | The postal code of the practice location | Yes | 01234 (if the NPI is entered this field will be pulled from there) |
| Phone | The phone number of the practice | Yes | 123-456-7890 (if the NPI is entered this field will be pulled from there) |
| Fax | The fax number of the practice | No | 098-765-4321 (if the NPI is entered this field will be pulled from there) |
| ID 1 Type | The type of the first identity document submitted for this user | Yes | passport |
| ID 2 Type | The type of the second identity document submitted for this user | Yes | state id |

Once every user in the CSV has these fields satisfied, the Admin which will prompt a file dialog where they can select the CSV. After selection they can select the **Submit** button to submit the CSV for validation. See *Figure 36 – Submitting a CSV* and the instructions that coincide with it on page 71 for information regarding the submission process.

All users that have been added to the portal shall be notified via an email sent to the Notification Email specified in the CSV (unless the Password field was specified). Once the users have been provisioned they shall be able to send and receive Direct messages.

## Bulk Import for users covered by Patient certificates

Users that are covered by patient certificates have a different set of requirements, and are generally not granted the same privileges as those users who are covered under address or organization certificates. This is because these users are actual patients of healthcare providers, and thus do not require the same capabilities as a provider on the portal. HCO users generally do not want their patients to have access to their employee portal, and have an entirely separate patient portal for their patient users in most cases.

The Admin should gather all necessary information to insert into the CSV that needs to be generated to make the upload process go smoothly. While less fields are required for patients to be added, there is no NPI available for them which makes certain fields require manual entry for all users.

To ensure that the CSV entered by the Admin user is valid upon upload, refer to the table below to properly structure the CSV. Note that two types of valid identity documents must be stated in the CSV since address certificates are being used. The actual documents themselves are not required in the CSV itself. Simply stating what type of document (i.e. Driver's License) will suffice.

**Table 5 – CSV structure for Bulk Upload (Patient Certificates)**

| Field | Description | Required Field? | Output Example |
|---|---|---|---|
| Direct Messaging Address | The Direct Address of the user | Yes | jsmith@direct.test.com |
| First Name | The user's first name | Yes | Fred |
| Middle Name | The user's middle name | No | |
| Last Name | The user's last name | Yes | Smith |
| Suffix | The suffix of the user | No | |
| Notification Email | Email address where the user shall receive all of their notifications | Yes | fs@gmail.com |
| Password | The password of the user being added. This prevents account registration notifications from being sent. | No | P@55word |
| User ID | The ID of the user to be | No | Test User |

| | | | |
|---|---|---|---|
| | displayed on the Direct Messaging Portal | | |
| Optional Field 1 | This field does not provide information | No | |
| Address (Line 1) | The Address line 1 of the practice location | Yes | 1 Town Rd (if the NPI is entered this field will be pulled from there) |
| Address (Line 2) | The Address line 2 of the practice location | Yes | Suite 204 (if the NPI is entered this field will be pulled from there) |
| City | The city of the practice location | Yes | NewCity (if the NPI is entered this field will be pulled from there) |
| State Province Code | The state of the practice location | Yes | AK (If the NPI is entered this field will be pulled from there) |
| Postal Code | The postal code of the practice location | Yes | 01234 (if the NPI is entered this field will be pulled from there) |
| ID 1 Type | The type of the first identity document submitted for this user | Yes | Drivers License |
| ID 2 Type | The type of the second identity document submitted for this user | Yes | State ID |

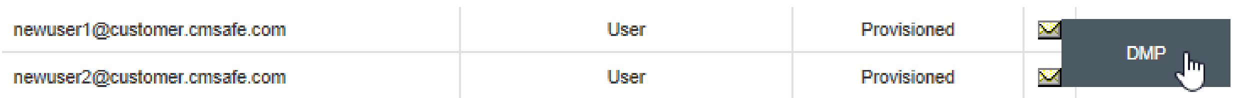
Once every user in the CSV has these fields satisfied, the TA can select Upload which will prompt a file dialog where they can select the CSV. After selection they can select the **Submit** button to submit the CSV for validation. See *Figure 36 – Submitting a CSV* and the instructions that coincide with it on page 71 for information regarding the submission process.

All added users shall be notified via an email sent to their Notification Address specified in the CSV (unless the Password field was specified). Since these users fall under the patient user type, the Admin or TA who added them, shall be responsible for administrating them.

## RE-SENDING NOTIFICATIONS (RETRY PROVISIONING)

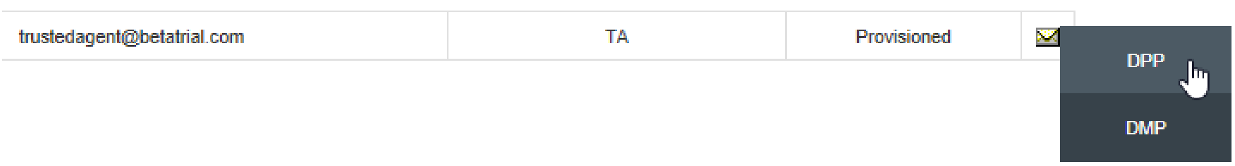
If a user fails to provision or if they never receive or delete the original account registration email notification, an option exists which allows an Admin to send out a new notification to the user. This is accomplished by following the steps below:

1. On the Home page, click on the Users tab.
2. Find the user to re-send the notification to and hover over the icon.
3. You should see a small popup that looks like the following:




4. Click on DMP to send a new notification to the user.

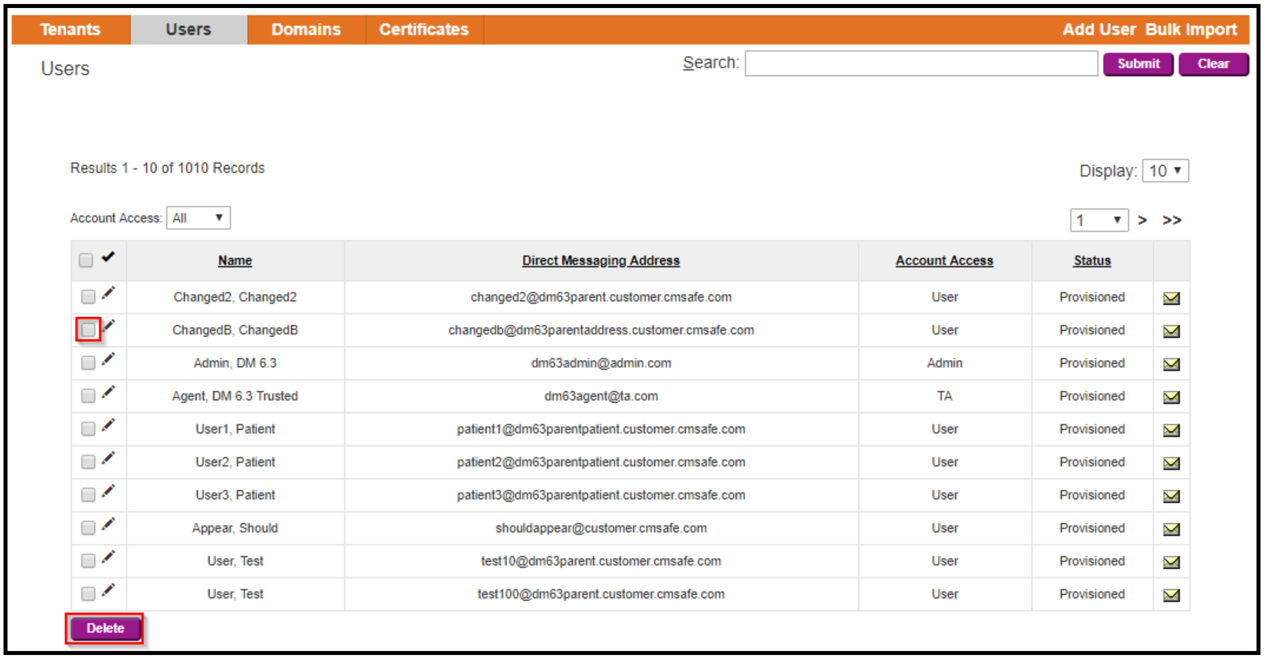
If an Administrator or TA requires a new notification be sent to them the same steps apply as listed above. The only difference is that instead of selecting the DMP option there will be a DPP option which must be clicked instead. See
below:




## DELETING USERS

An Admin can delete all types of users from the web portal and CA/RA if desired. These actions cannot be undone once committed. The only thing that can be done is to completely re-add the organizations, users, or both. No data that was contained in the user's accounts shall be restored if they are re-added after deletion, so ensure that any sensitive or important data is stored somewhere before deleting a user. The actual process itself for deleting a user is the same for every user type, and is described below.

1. On the Home page, click on the Users tab.
2. Find the user you want to delete and click the respective checkbox.
3. More than a single user can be deleted at once by clicking additional checkboxes.




4. The user will be put into Awaiting Delete status for a few seconds before being completely removed.

## DELETING A TRUSTED AGENT

While an Admin has the capability to delete a TA, non-TA Admin, or Direct User if required, it should be noted that these actions are permanent, and require that different actions be taken depending on the type of user deleted.

If a TA user is deleted the certificates that were generated under their name for Direct users will not be lost. All that is required is for a new TA to be named on the certificates in order for the certificates to remain active. If no TA is named on the certificates it will not be possible to continue using them. It is advised that a new TA be named on these certificates as soon as possible, if not immediately to avoid this scenario.

Please note that if a TA is covered under an Address Certificate, it should be revoked.

## DELETING DIRECT USERS

Unlike deleting a TA user, deletion of a Direct User causes the certificate that was in their possession to be rendered invalid. When this happens the certificate must be revoked. For details on how the revocation process is handled see the *Revoking a Certificate* section.

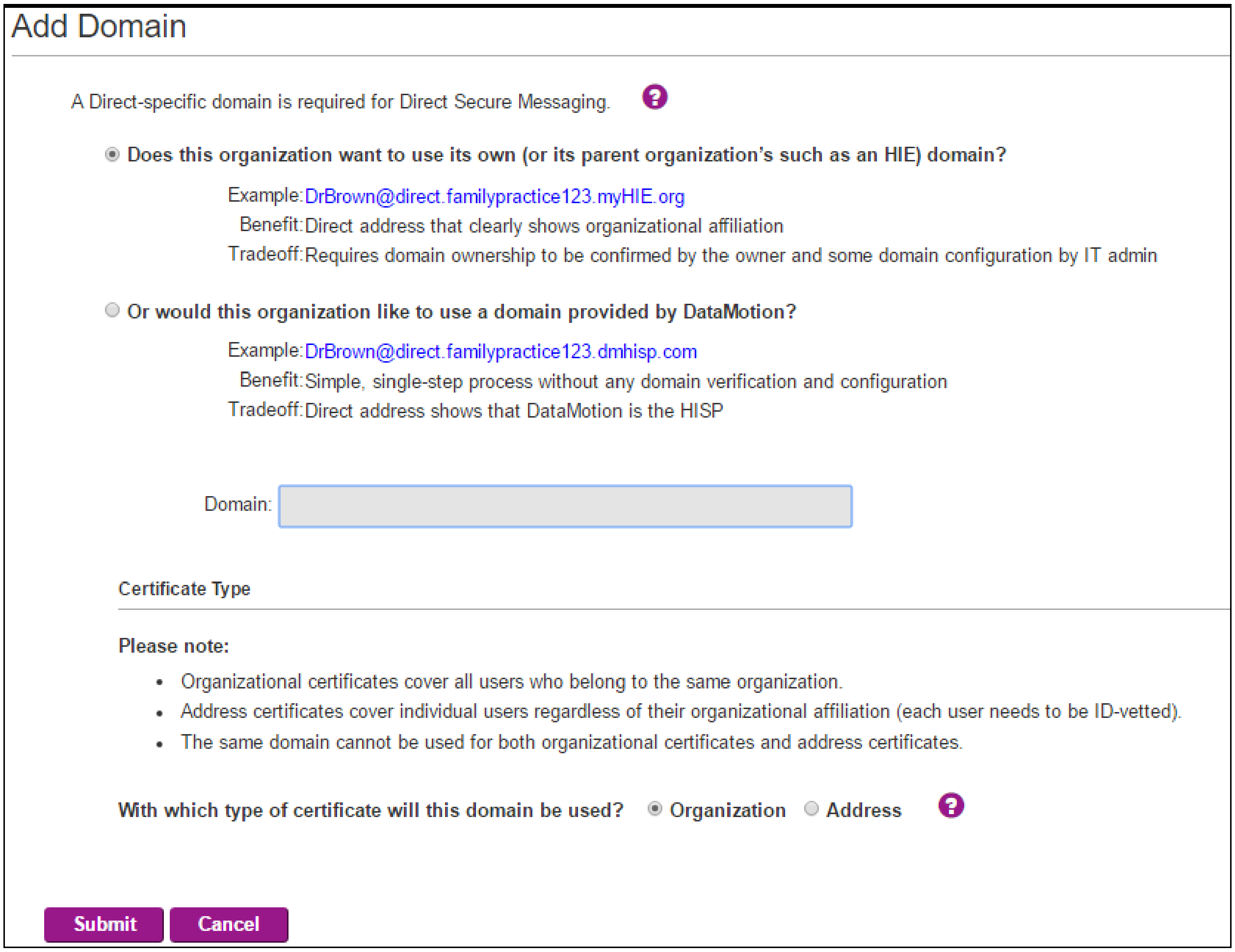
## DELETING A NON-TA ADMINISTRATOR

Deleting a Non-TA Administrator will not require a certificate to be revoked like in the case of deleting a TA and Direct User (covered by address certificate). If this is the case see the *Revoking a Certificate* section for more information on how to revoke a certificate.

## ADDING AND VALIDATING A DOMAIN

Validating your domain is essential to accessing all of the features contained within the DPP such as certificate requests for users, and adding additional Direct users to companies. In order to validate your domain, you must have the HCO in question enrolled on the DataMotion Portal (see the section *Provision a Tenant Organization* on page 31 and its three subsequent sections for information on how to perform this task). Domain type restrictions must also be set by the HCO's parent. Detailed steps to perform domain validation are listed below.

**Figure 37 – Validating an organization's domain**




1. Select Yes or No to add a domain to the DPP. Selecting Yes will display the options available.

   » Decide whether or not you want to use a domain of your own choosing by selecting the first radio button, or if you want to use a DataMotion domain by selecting the second radio button.

   **NOTE: If you choose to use a DataMotion domain it will not be possible to select Organization as the Certificate Type.**

2. Enter the name of the domain you want in the Domain field.
3. Select the Certificate type, either Organization or Address is available.
4. Click Next to continue.

The domain will be fully registered with the DataMotion CA/RA and the web portal. Any additional domains that are created and validated will not replace any previously registered domains. All steps must be completed again for any additional domains that you wish to add.

Any time that you submit a domain for validation, the portal will keep a record of the submission and keep a status record of them on the **Domains** tab. If you navigate to this tab, you can view the day and time the submission was sent, applicant name, domain admin email address, and all other important information concerning your submissions.

## EDITING AN HCO

It is commonplace for any organization to have staff or general company changes over time. Healthcare Organizations are not an exception to this rule, and as a result, the DPP allows administrators to edit certain fields of an HCO that they oversee at any time. Depending on the level of the administrator within the hierarchy, it may be possible for them to edit any of the HCOs in the tree or only a select few.

Some fields may not be changed by using the editing screen. This includes the following:

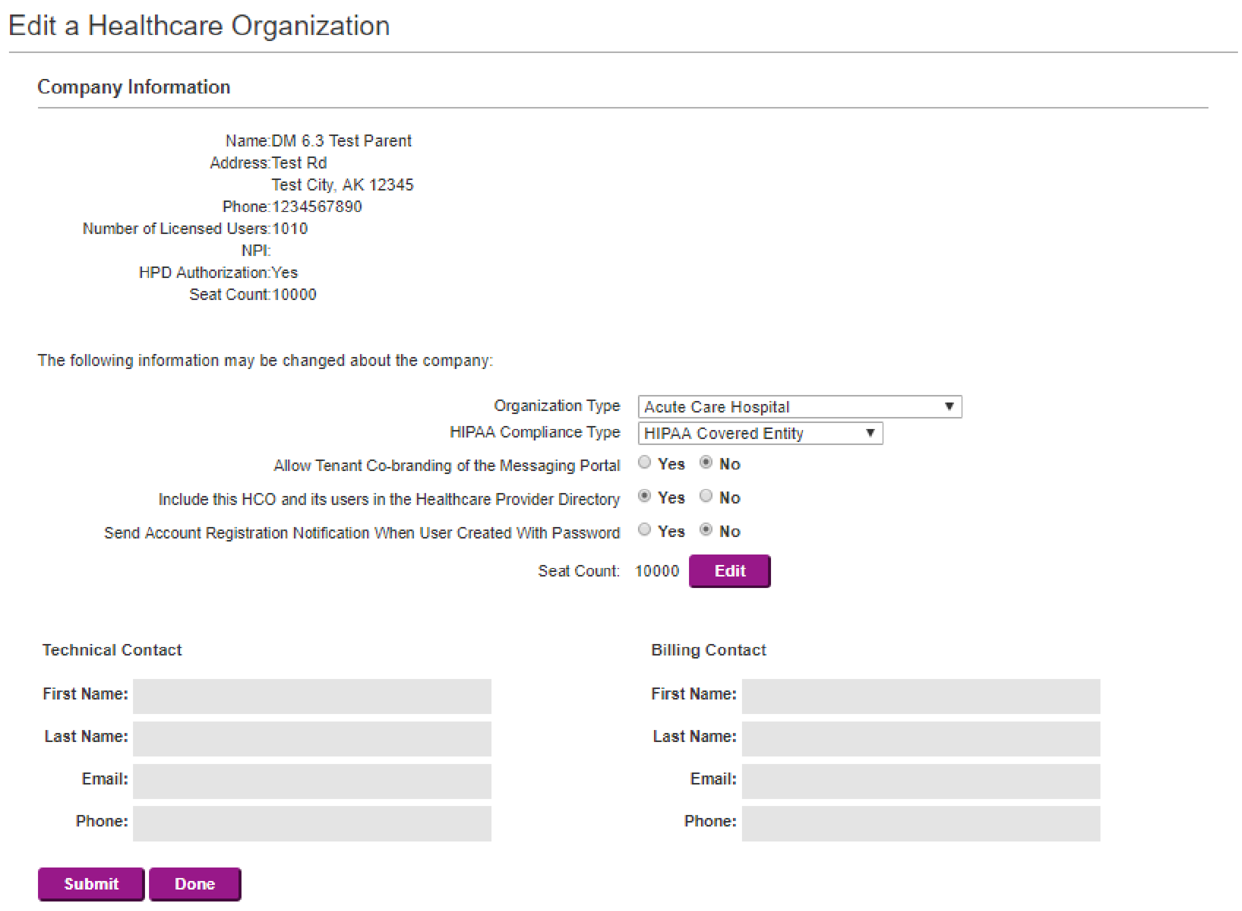
- **Name:** (the name of the HCO)
- **Address:**
- **Phone:**
- **NPI:**
- **Organization Type:**
- **HIPAA Compliance:**

To access the editing page and change an HCO's information, perform the steps listed below.

1. On the Home page of the DPP, click the **Edit Org** button.


2. Perform any edits to the HCO that you desire which includes the following:
   » **Allow Tenant Co-branding of the Messaging Portal**. Setting this field to Yes will allow administrators of tenants in child organizations to set cobrands for their own portals.
   » **Include this HCO and its users in the Healthcare Provider Directory**. If your HCO already has its HPD Authorization set to Yes, then setting this field to No will remove the all of the users and the HCO itself from the HPD. If the HPD Authorization setting is No, then setting this field to Yes will add the HCO and all of its users to the HPD.
   » **Technical Contact**. If a Technical Contact was not set during HCO creation, and you wish to create one, set all four fields to some value. Failure to do so will result in an error. Changing who the contact is follows the same instructions. If you do not want a contact to be set here simply leave all of the fields blank.
   » **Billing Contact**. If a Billing Contact was not set during HCO creation and you wish to create one, set all four of the fields to some value. Failure to do so will result in an error. Changing who the contact is follows the same instructions. If you do not want a contact to be set here simply leave all of the fields blank.
3. Click Submit to make the changes.

**Figure 38 – Edit a Healthcare Organization page**



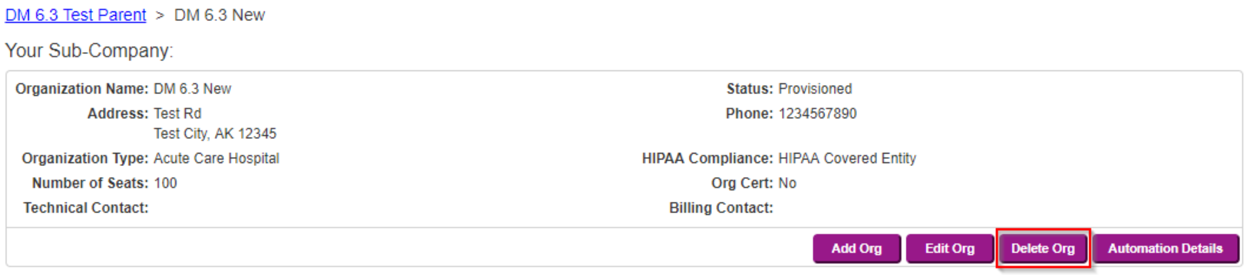

**NOTE: No prompt will be displayed that indicates the changes have been made, however if you click Done, you will notice that any changes you made will be displayed in the appropriate fields on the Home page.**

## DELETING AN ORGANIZATION

Organizations can be deleted if the HCO no longer requires a tenant to be covered beneath it. Caution is advised in this case as deleting an organization shall remove all users from the portal and the DataMotion CA/RA. Take note that only companies below your level in the hierarchy can be deleted. You cannot delete the organization that you currently are a part of.

**NOTE: If an organization has tenants of its own beneath it in the hierarchy then they must be deleted first starting at the lowest level.**

**Figure 39 – Deleting an organization**




1. On the Home page click the Delete Org button.
2. A prompt will display asking if you wish to continue, click OK.
3. Deletion will be near instantaneous, and you will be placed in the Home page of the tenant organization.

Once the organization has been removed, the admin will be notified via their method of choice.

## ADDING AND REGISTERING CHILD ORGANIZATIONS

An Admin is able to create additional organizations in the hierarchy using the same method as described in the Provision a Tenant Organization section. The key difference that separates adding a child organization is highlighted in the following sections.

### ADDING A CHILD ORGANIZATION

When an Admin creates an organization designated to be a child of the parent, they can generally follow the same steps listed in throughout the Create Organization section. During this process it is still possible for a TA user to be created at the new HCO despite a regular Admin lacking TA privileges. This is due to the validation process being outside of the Admin's control, thereby eliminating any risk to security or compliance.

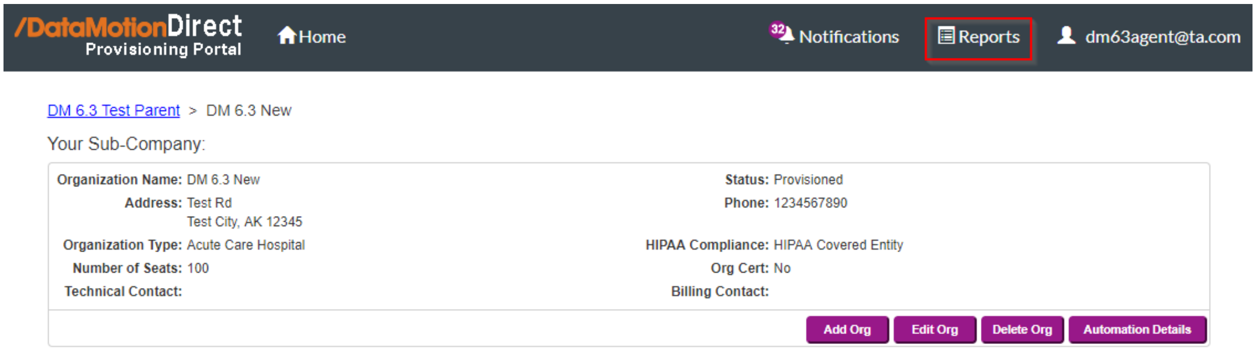
**NOTE: It is not recommended to create a company and leave it without a TA since it will not be possible to perform certificate requests without one.**

## REPORTS AND LOGGING

Many of the actions taken on the portal will be logged and retained for future reference and auditing purposes. Admin users on the portal will have access to these reports, and can generate them at any time. Certain reports can be run against a certain date/time range selectable by month, quarter, year or a range of dates going back to January first of the previous year.

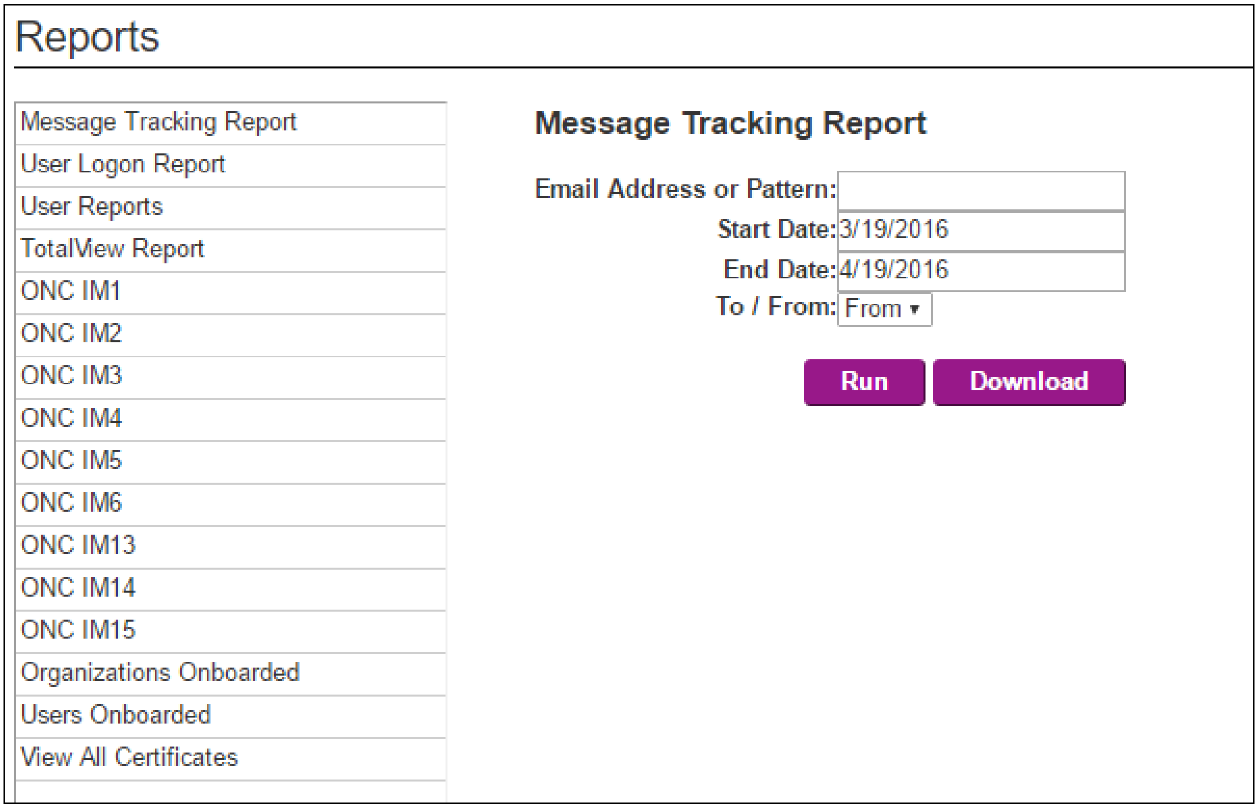
To access the Reports page perform the following steps:

1. On the Home page, click the Reports link in the navigation bar.




2. The side panel on the left side of the screen contains all of the reports available to you.

**Figure 40 – Reports page**




The Message Tracking Report is always the first to be shown whenever the Reports page loads.

Note that some of the reports can be generated and displayed on the web portal itself, while some others must be downloaded. The reports that must be downloaded, generally contain more information than a web page can properly display.

> **NOTE: All reports are downloaded as .csv files. These files are best opened and viewed in a spreadsheet software such as Microsoft Excel. If you do not have Excel a free alternative such as Google Docs will also suffice.**

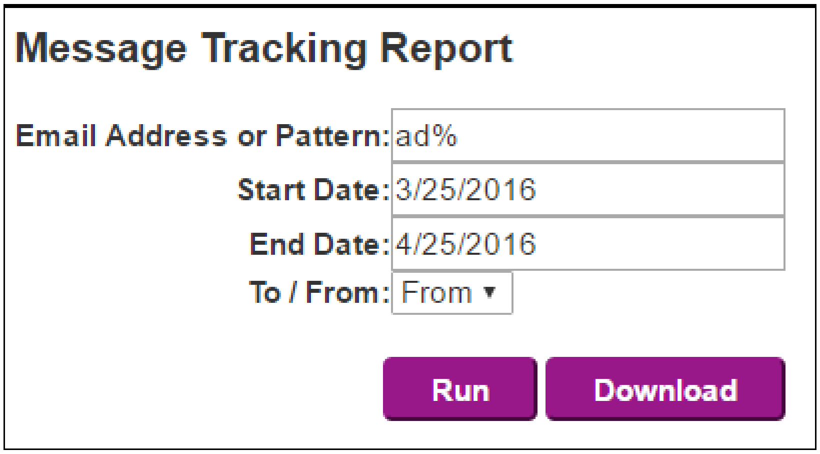
The following sections describe the reports that are available to admin users on the portal.

## MESSAGE TRACKING REPORT

The message tracking report allows you to search for messages based on pattern matching. The search will look at the message addresses and subject lines to find the matches (message bodies are not searched).

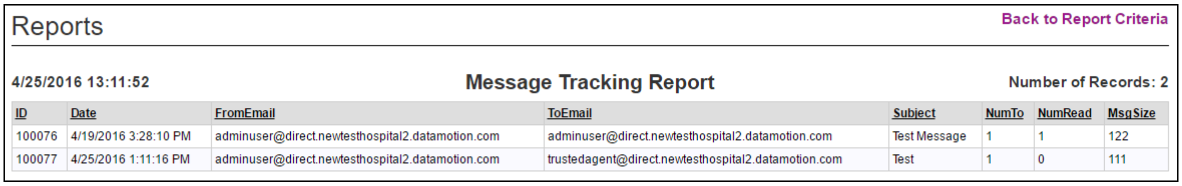
To generate a Message Tracking Report perform the following steps:

1. Click the Message Tracking Report link from the side panel.
2. Enter the search parameters into the Email Address or Pattern field, and the Start and End Date fields. The To / From field specifies whether to search for the Email Address or Pattern in the Message To or the From field.




3. Click Run or Download to generate the report.

**Figure 41 – Message Tracking Report Results**


Reports
Back to Report Criteria

4/25/2016 13:11:52 Message Tracking Report Number of Records: 2

| ID | Date | FromEmail | ToEmail | Subject | NumTo | NumRead | MsgSize |
|---|---|---|---|---|---|---|---|
| 100076 | 4/19/2016 3:28:10 PM | adminuser@direct.newtesthospital2.datamotion.com | adminuser@direct.newtesthospital2.datamotion.com | Test Message | 1 | 1 | 122 |
| 100077 | 4/25/2016 1:11:16 PM | adminuser@direct.newtesthospital2.datamotion.com | trustedagent@direct.newtesthospital2.datamotion.com | Test | 1 | 0 | 111 |

The report displays all the messages matching the specified criteria.

## USER LOGON REPORT

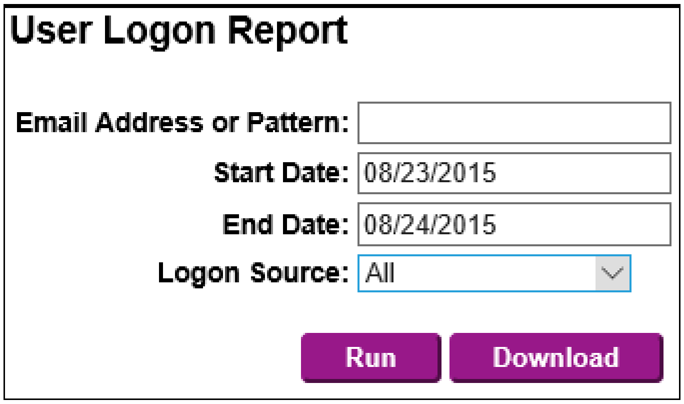
The User Logon Report generates reports about user logon activity. You can look at activity for specific users, defined timeframes and also how the user logged into the service.

To generate a User Logon Report perform the following steps:

1. On the Reports page, click the User Logon Report from the side panel.
2. Enter the search parameters into the Email Address or Pattern field, and the Start and End Date fields. The Logon Source field specifies which service the user accessed. The

default selection is All which will show every service the user has used. Specifying which service to check for is also possible. You will be provided with the following choices.

- Web
- POP3
- CMLFT
- ContactUs
- DirectoryService
- CmV4
- ThirdParty
- SendSecureButton
- SFTP
- SingleSignOn




3. Click Run or Download to generate the report.

**Figure 42 – User Logon Report Results**

Reports

Back to Report Criteria

4/25/2016 13:13:03

**User Logon Report**

Number of Records: 113

| Date | Email | FName | LName | Source | IP | Status |
|---|---|---|---|---|---|---|
| 4/25/2016 1:13:03 PM | adminuser@direct.newtesthospital2.datamotion.com | Admin1 | User1 | SingleSignOn | 10.0.0.155 | Success |
| 4/25/2016 1:11:52 PM | adminuser@direct.newtesthospital2.datamotion.com | Admin1 | User1 | SingleSignOn | 10.0.0.155 | Success |
| 4/25/2016 1:10:35 PM | adminuser@direct.newtesthospital2.datamotion.com | Admin1 | User1 | Web | 192.168.10.151 | Success |
| 4/25/2016 1:09:43 PM | adminuser@direct.newtesthospital2.datamotion.com | Admin1 | User1 | Unknown | | Success |
| 4/25/2016 12:38:19 PM | adminuser@direct.newtesthospital2.datamotion.com | Admin1 | User1 | Unknown | | Success |
| 4/25/2016 12:38:15 PM | adminuser@direct.newtesthospital2.datamotion.com | Admin1 | User1 | Unknown | | Invalid |
| 4/22/2016 3:55:59 PM | johndoe16@testcompany.direct.med.com | John | Doe | Unknown | | Success |
| 4/22/2016 3:55:15 PM | Dpp_23ba693fd39543cb8de5b8aa9ee1f675@datamotion.com | | | SingleSignOn | 10.0.0.155 | Success |
| 4/22/2016 3:54:58 PM | Dpp_23ba693fd39543cb8de5b8aa9ee1f675@datamotion.com | | | SingleSignOn | 10.0.0.155 | Success |
| 4/22/2016 1:46:52 PM | adminuser@direct.newtesthospital2.datamotion.com | Admin1 | User1 | Unknown | | Success |
| 4/22/2016 1:05:58 PM | adminuser@direct.newtesthospital2.datamotion.com | Admin1 | User1 | Unknown | | Success |
| 4/22/2016 11:37:21 AM | adminuser@direct.newtesthospital2.datamotion.com | Admin1 | User1 | Unknown | | Success |
| 4/22/2016 11:09:12 AM | adminuser@direct.newtesthospital2.datamotion.com | Admin1 | User1 | Unknown | | Success |
| 4/22/2016 10:52:24 AM | adminuser@direct.newtesthospital2.datamotion.com | Admin1 | User1 | Unknown | | Success |
| 4/22/2016 10:36:00 AM | adminuser@direct.newtesthospital2.datamotion.com | Admin1 | User1 | Unknown | | Success |
| 4/21/2016 5:02:04 PM | adminuser@direct.newtesthospital2.datamotion.com | Admin1 | User1 | Unknown | | Success |
| 4/21/2016 4:02:50 PM | trustedagent@direct.newtesthospital2.datamotion.com | Trusted1 | Agent1 | Unknown | | Success |
| 4/21/2016 3:54:52 PM | trustedagent@direct.newtesthospital2.datamotion.com | Trusted1 | Agent1 | Unknown | | Success |

The report displays all the logon events for the user based on the specified criteria.

## USER REPORTS

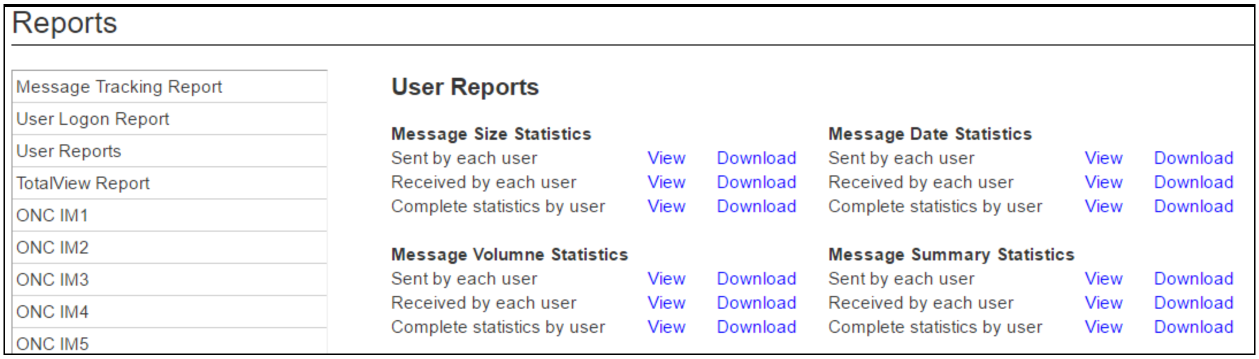
There are several types of user reports, each of which can be filtered for sent or received messages (or both) for each user. These reports are summaries of user statistics as compared to the more detailed Message Tracking Report.

**Table 6 – User Report Type Descriptions**

| Report Type | Description |
|---|---|
| Message Size Statistics | Shows the size of messages sent and received by each user. |
| Message Date Statistics | Shows when messages have been sent by the users (first and last messages for each user). |
| Message Volume Statistics | Shows the number of messages sent/received by the user. |
| Message Summary Statistics | Shows the fields of the other statistics reports on one screen. |

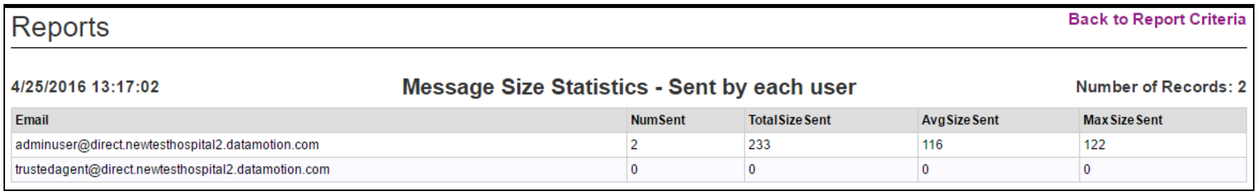
To generate any of the User Reports perform the following steps:

1. On the Reports page click the User Reports link on the side panel.




2. Click on the Report to be shown, for example: Message Size Statistics: Sent by each user:

**Figure 43 – User Reports Type Result**




| Email | NumSent | TotalSizeSent | AvgSizeSent | MaxSizeSent |
|---|---|---|---|---|
| adminuser@direct.newtesthospital2.datamotion.com | 2 | 233 | 116 | 122 |
| trustedagent@direct.newtesthospital2.datamotion.com | 0 | 0 | 0 | 0 |

## TOTAL VIEW REPORT

The TotalView Report provides complete tracking of all messages. The report contains a record of every message sent along with the tracking data for the message and any attachments in a single report. This report is provided as a CSV file which can be evaluated in other programs, such as Microsoft Excel.

The TotalView report includes the following fields:

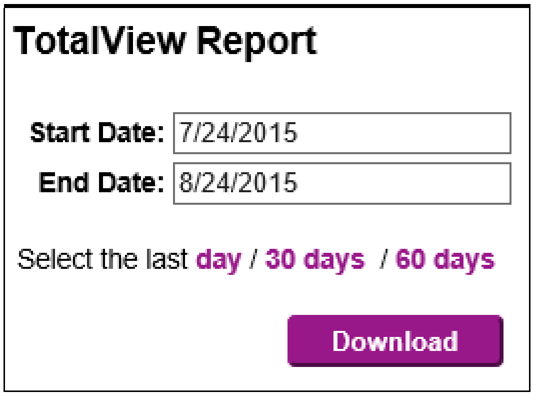
- Message ID
- Custom ID
- Date
- From Email
- To Email
- Subject
- Notification TimeStamp
- Notification Type
- Message Status
- Message Open Time
- Attachment Name
- Attachment Size
- Attachment Status

- Attachment Open Time

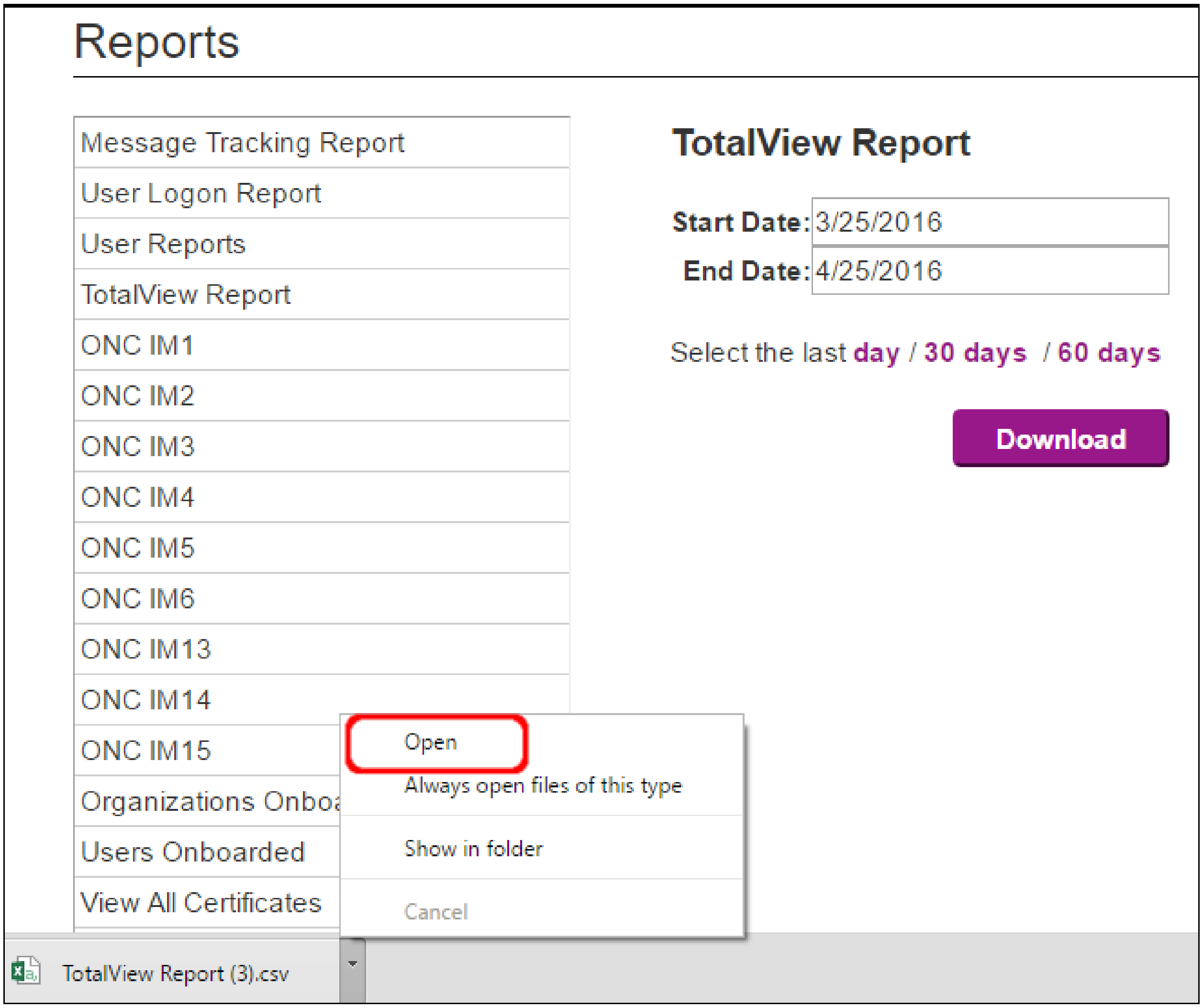
Each message and every attachment within a message is reported individually For example, a message to two recipients with two attachments will generate four rows of data, two for each recipient, with one attachment listed on each line per recipient.

To generate a TotalView Report perform the following steps:

1. On the Reports page click the TotalView Report link on the side panel.
2. Specify the Date range for the report.
   » There are quick options for the last **day**, **30 days**, and **60 days** below the standard Date fields. These will automatically select the specified time period.




3. Click Download to generate the report. The report itself will be downloaded to the machine being used to view the portal.




## ONC REPORTS

DataMotion has included tracking data that allows all admin users the capability to generate them at will. These reports are essential to sending the proper information to the ONC should the need ever arise for the information to be sent to the ONC.

Options available for generating ONC reports have been made available to provide HCOs with an easier way to collect data regarding their organization's activities. Some reports that cover sections of the ONC are unavailable for generation on the portal. This is not a limitation of the portal. DataMotion simply does not collect information regarding certain areas of information to properly form reports that would satisfy their criteria.

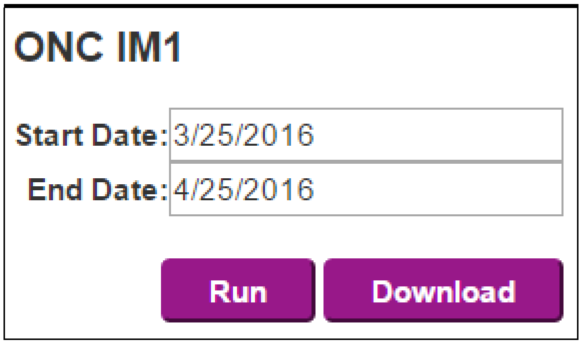
The available reports are described in the following sections.

## IM1

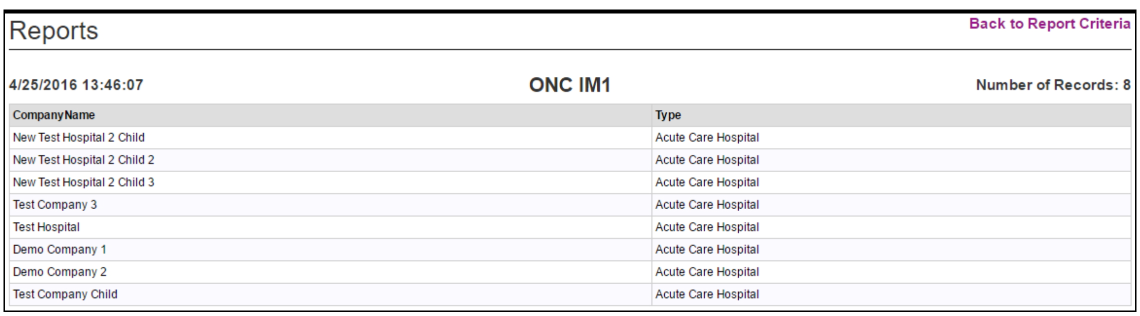
Shows the details of the organizations that are enabled for direct exchange. Any subtenants that were created for the tenant company will be included in the report's information.

To generate an IM1 report perform the following steps:

1. On the Reports page click ONC IM1 from the side panel.
2. Enter the Start and End Date range for the report.




3. Click either Run or Download to retrieve the report. The report displays all of the company names and their corresponding organization type if they have been enabled for Direct exchange. The following is a sample of what the report will look like.



Reports | Back to Report Criteria

4/25/2016 13:46:07 | ONC IM1 | Number of Records: 8

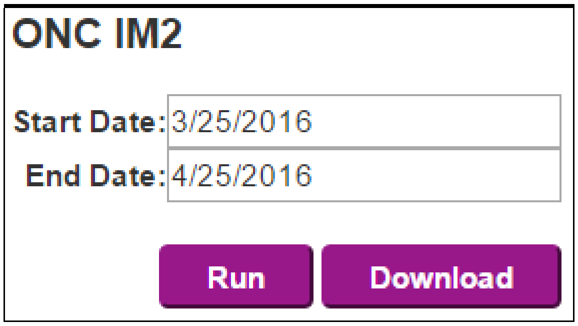
| CompanyName | Type |
|---|---|
| New Test Hospital 2 Child | Acute Care Hospital |
| New Test Hospital 2 Child 2 | Acute Care Hospital |
| New Test Hospital 2 Child 3 | Acute Care Hospital |
| Test Company 3 | Acute Care Hospital |
| Test Hospital | Acute Care Hospital |
| Demo Company 1 | Acute Care Hospital |
| Demo Company 2 | Acute Care Hospital |
| Test Company Child | Acute Care Hospital |

## IM2

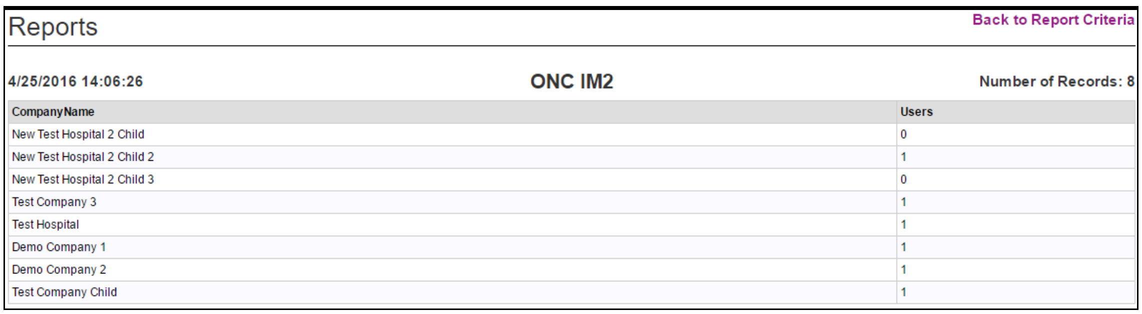
Shows the individual users of the HCO that are Direct enabled. Any subtenants that are included and below the administrator on the tree, are displayed in the results as well.

To generate an IM2 report perform the following steps:

1. On the Reports page click ONC IM2 from the side panel.
2. Enter the Start and End Date.




3. Click either Run or Download to retrieve the report. The report displays all of the users that are at the same level or below them in the hierarchy. The following is a sample of what the report will look like.



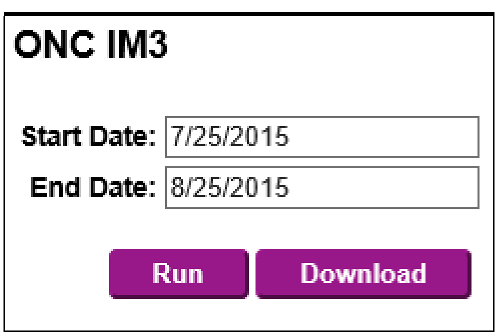

| CompanyName | Users |
|---|---|
| New Test Hospital 2 Child | 0 |
| New Test Hospital 2 Child 2 | 1 |
| New Test Hospital 2 Child 3 | 0 |
| Test Company 3 | 1 |
| Test Hospital | 1 |
| Demo Company 1 | 1 |
| Demo Company 2 | 1 |
| Test Company Child | 1 |

## IM3

Shows the Acute Care Hospitals that are a part of the HCO and enabled for Direct exchange. Only hospitals that have sent or received at least a single message will appear in the results.

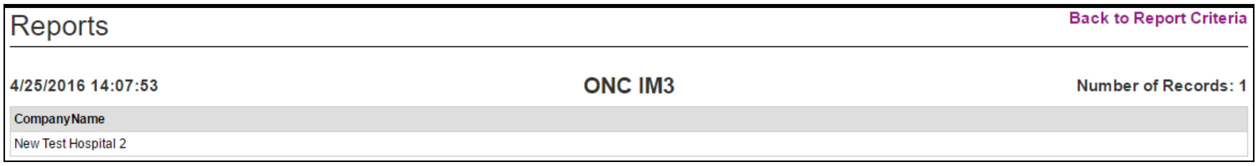
To generate an IM3 report perform the following steps:

1. On the Reports page click ONC IM3 from the side panel.
2. Enter the Start and End Date.




3. Click either Run or Download to retrieve the report. The report displays the company name of all Acute Care Hospital company types. If your HCO does not

contain any subtenants created on the portal with this company type, no information will be displayed.

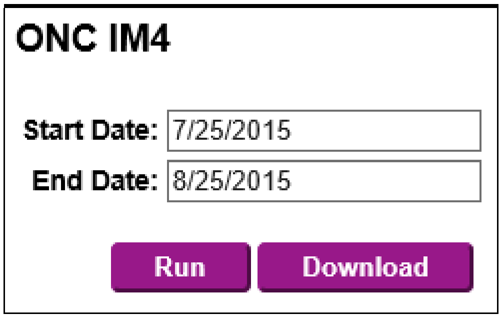



## IM4

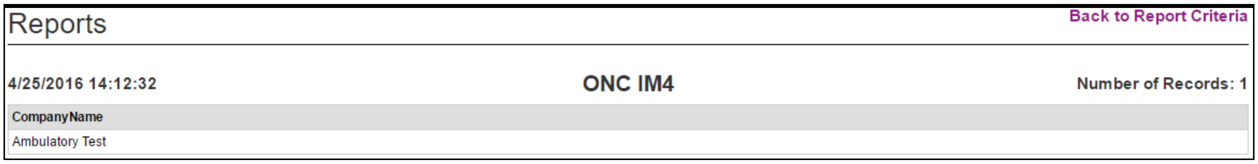
Shows the Ambulatory entities that are a part of the HCO and enabled for Direct exchange. Only entities that have sent or received at least a single message will appear in the results.

To generate an IM4 report perform the following steps.

1. On the Reports page click ONC IM4 from the side panel.
2. Enter the Start and End Date.




3. Click either Run or Download to generate the report. The report displays the company name of all Ambulatory entities. If your HCO does not contain any subtenants created on the portal with this company type, no information will be displayed.

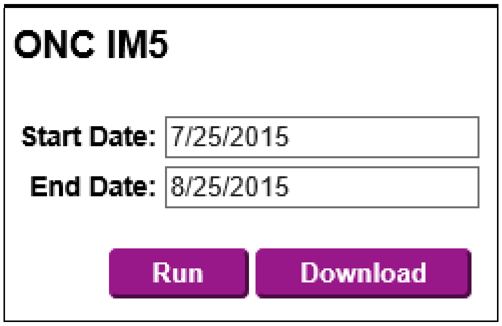



## IM5

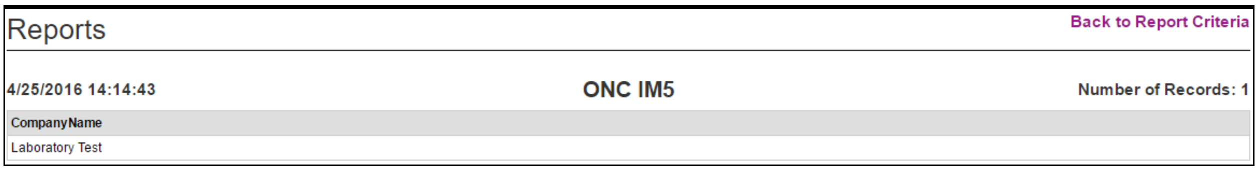
Shows the Laboratory based companies that are a part of the HCO and enabled for Direct exchange.

To generate an IM5 report perform the following steps.

1. On the Reports page click ONC IM5 from the side panel.
2. Enter the Start and End Date.




3. Click either Run or Download to generate the report. The report displays the company name of all Laboratories. If your HCO does not contain any subtenant created on the portal with this company type, no information will be displayed.


Reports — Back to Report Criteria

4/25/2016 14:14:43 — ONC IM5 — Number of Records: 1

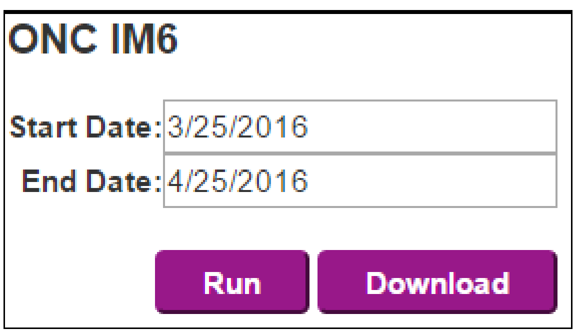
| CompanyName |
|---|
| Laboratory Test |

## IM6

Shows any companies that are not registered on the portal as a pre-defined organization type. These companies must have either sent or received a Direct message after being provisioned to appear in the results.

To generate an IM6 report perform the following steps.

1. On the Reports page click ONC IM6 from the side panel.
2. Enter the Start and End Date.



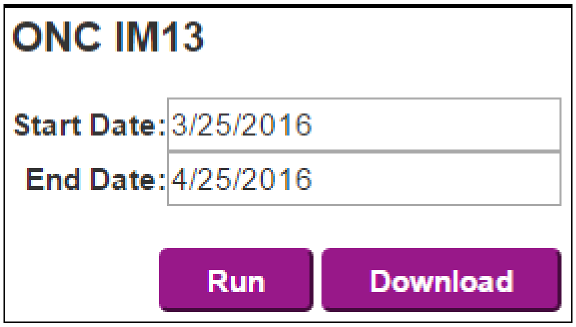

3. Click either Run or Download to generate the report. The report displays the company name for all of the companies that fall outside of the pre-defined organization types. If your HCO only has subtenants that fall under the pre-defined categories, no information will be displayed.

## IM13

Shows all Direct based transactions for the tenant and its subtenants. The transactions are considered to be any Direct message sent or received by a company's users within the HCO.

To generate an IM13 report perform the following steps.

1. On the Reports page click ONC IM13 from the side panel.
2. Enter the Start and End Date.




3. Click either Run or Download to generate the report. The report displays the company name and the number of Direct messages sent or received for all of the companies.

Reports — Back to Report Criteria

4/25/2016 14:17:38 — **ONC IM13** — Number of Records: 4

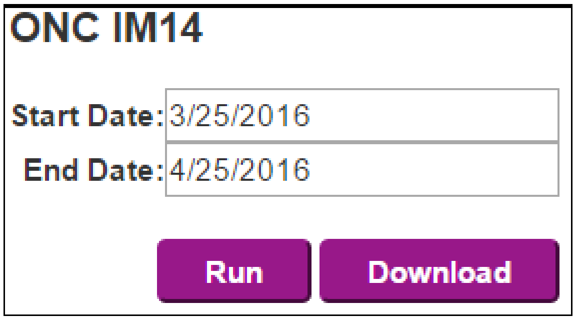
| CompanyName | NumberSent | NumberReceived |
|---|---|---|
| New Test Hospital 2 | 2 | 2 |
| New Test Hospital 2 Child | 0 | 0 |
| New Test Hospital 2 Child 2 | 0 | 0 |
| Test Company Child | 0 | 0 |

## IM14

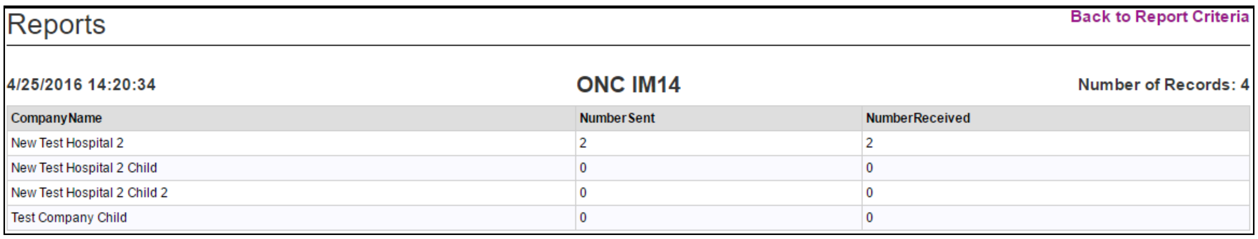
Shows all Direct transactions from/to hospital or ambulatory entity company types that are either tenants or subtenants within the HCO.

To generate an IM14 report perform the following steps.

1. On the Reports page click ONC IM14 from the side panel.
2. Enter the Start and End Date.




3. Click either Run or Download to generate the report. The report displays the company name and the number of Direct messages sent or received so long as the transaction took place from/to a hospital or an ambulatory entity.


Reports
Back to Report Criteria

4/25/2016 14:20:34 ONC IM14 Number of Records: 4

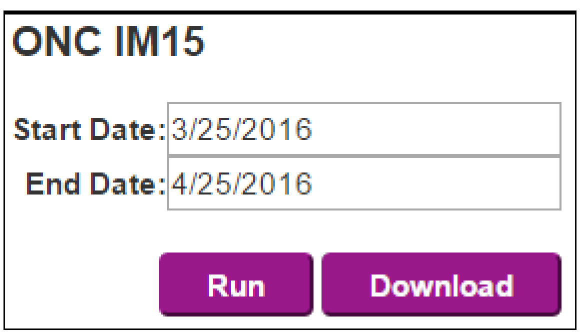
| CompanyName | NumberSent | NumberReceived |
|---|---|---|
| New Test Hospital 2 | 2 | 2 |
| New Test Hospital 2 Child | 0 | 0 |
| New Test Hospital 2 Child 2 | 0 | 0 |
| Test Company Child | 0 | 0 |

## IM15

Shows all Direct transactions performed by clinical laboratories within the HCO. This includes messages sent from and to the laboratories.

To generate an IM15 report perform the following steps.

1. On the Reports page click ONC IM15 from the side panel.
2. Enter the Start and End Date.



3. Click either Run or Download to generate the report. The report displays the company name of the clinical laboratory and the number of Direct messages sent or received by that company.

Reports

Back to Report Criteria

4/25/2016 14:44:23 ONC IM15 Number of Records: 4

| CompanyName | NumberSent | NumberReceived |
|---|---|---|
| Laboratory Test | 0 | 0 |

## ONBOARDING REPORTS

The portal will record all of the information that an administrator puts into the portal when onboarding organizations and users. This information can be downloaded as a CSV file to any storage drive available on the machine the admin is using.

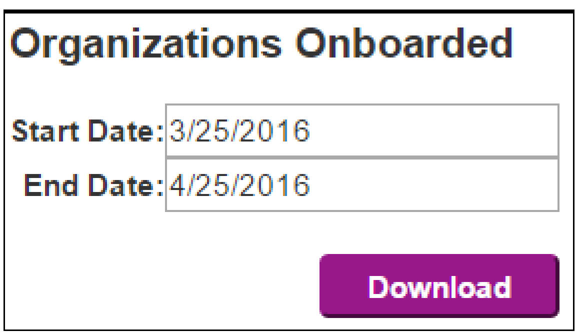
### Organizations Onboarded

All information that is entered into the portal by an administrator during the process of creating an organization. This information will be represented in a table format whenever the report is downloaded.

To generate an Organizations Onboarded report, perform the following steps.

1. On the Reports page click Organizations Onboarded from the side panel.

2. Enter a Start and End Date.




3. Click Download.

The CSV file will look like the following.

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Organizations Onboarded | | | | | | | | | | | | | | |
| 2 | | | | | | | | | | | | | | | |
| 3 | OrgName | OrgType | SoleProprietor | Address | Address2 | City | State | Zip | Country | Domain | OncUserType | MuUserTy | LoA | NumberO | DateAdded |
| 4 | New Test | Acute Care Hospital | No | 1 Test Rd | | Test City | AK | 1234 | United Sta | direct.new | Clinical | EP | | 1000 | 4/7/2016 |
| 5 | New Test | Acute Care Hospital | No | 1 Test Rd | | Test City | AK | 1234 | United Sta | direct.new | Clinical | EP | | 3000 | 4/8/2016 |
| 6 | New Test | Acute Care Hospital | No | 1 Test Rd | | Test City | AK | 1234 | United Sta | direct.new | Clinical | EP | | 100 | ######### |
| 7 | New Test | Acute Care Hospital | No | | | | | | | direct.new | Non-Clinical | Non-EP | | 25 | ######### |
| 8 | Test Comp | Acute Care Hospital | No | | | | | | | direct.test | Non-Clinical | Non-EP | | 25 | ######### |
| 9 | Test Hosp | Acute Care Hospital | No | | | | | | | direct.testl | Non-Clinical | Non-EP | | 30 | ######### |
| 10 | Demo Cor | Acute Care Hospital | No | | | | | | | direct.dem | Non-Clinical | Non-EP | | 25 | ######### |
| 11 | Demo Cor | Acute Care Hospital | No | | | | | | | direct.dem | Non-Clinical | Non-EP | | 40 | ######### |
| 12 | Test Comp | Acute Care Hospital | No | New Company Street | | New Company City | AK | 7201 | United Sta | testcompa | Non-Clinical | Non-EP | | 15 | ######### |

All fields in the CSV will be shown whenever a report is downloaded. These fields include:

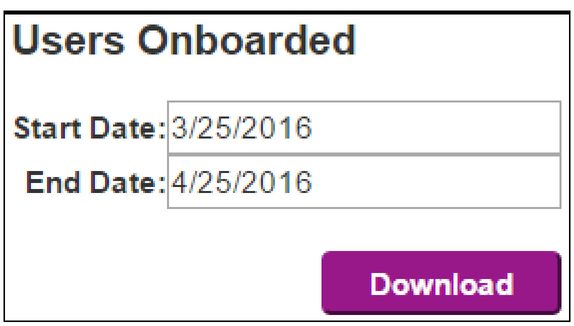
- OrgName
- OrgType
- SoleProprietor
- Address
- Address2
- City
- State
- Zip
- Country
- Domain
- OncUserType
- MuUserType
- LoA
- NumberOf Seats
- DateAdded

## Users Onboarded

When a user is on-boarded, all of the information entered into the portal is recorded so that it can be used for auditing purposes by your HCO. The information itself will be presented as a table when a report is downloaded.

To generate a User's Onboarded report, perform the following steps.

1. On the Reports page click Users Onboarded from the side panel.
2. Enter a Start and End Date.




3. Click Download.

The CSV file will look like the following.

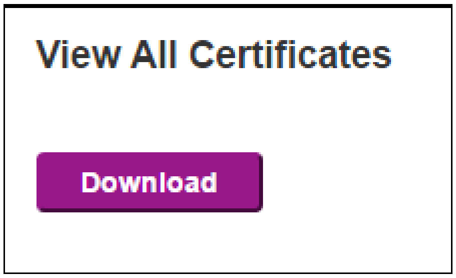
| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Users Onboarded | | | | | | | | | | | | | | | | | |
| 2 | | | | | | | | | | | | | | | | | | |
| 3 | Organizati | FirstName | LastName | Function | Address | Address2 | City | State | Zip | Country | Phone | ContactEn | DirectMes | CertType | Admin | TA | NPI | DateAdded |
| 4 | New Test | Trusted1 | Agent1 | | 1 Test Ave | | Test City | AK | 1234 | United States | | jsmith113 | trustedagent@direc | | No | Yes | | 4/7/2016 |
| 5 | New Test | Admin1 | User1 | | | | | AK | | United States | | kevinm@ | adminuser@direct.n | | Yes | No | | ######## |
| 6 | New Test | Bob | Smith | | | | | AK | | United States | | bsmith341 | bsmith4@direct.nev | | No | No | | ######## |
| 7 | New Test | Org1 | User1 | | | | | | | | | orguser@ | orguser@direct.new | | No | No | | ######## |
| 8 | New Test | Org1 | User1 | | | | | | | | | kevinm@ | orguser2@direct.ne | | No | No | | ######## |
| 9 | New Test | Org2 | User2 | | | | | | | | | kevinm@ | orguser3@direct.ne | | No | No | | ######## |
| 10 | New Test | Bob | Smith | | 3 | 3 | 3 | AK | 3 | | 3 | kevinm@ | mybulkaddressuser1 | | No | No | | ######## |
| 11 | New Test | Robert | Smith | | 4 | 4 | 4 | AK | 4 | | 4 | kevinm@ | mybulkaddressuser2 | | No | No | | ######## |
| 12 | New Test | Bob | Smith | | | | | AK | | United States | | bsmith341 | testuser@direct.nev | | No | No | | ######## |
| 13 | Test Comp | John | Doe | | 123 Testing Drive | | Testing | NH | 7746 | United States | | jsmith113 | johndoe16@testcon | | No | Yes | | ######## |

All fields in the CSV will be shown whenever a report is downloaded. These fields include:

- OrganizationName
- FirstName
- LastName
- Function
- Address
- Address2
- City
- State
- Zip
- Country
- Phone
- ContactEmail
- DirectMessagingAddress
- CertType
- Admin
- TA
- NPI
- DateAdded

## CERTIFICATE REPORT

The portal has the ability to display the certificates that each company possesses. It is only possible to download this report as an excel spreadsheet.




The result that will be returned will look something like the following:

| View All Certificates | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| CompanyName | Subject | Status | Representative | DateRequested | ExpirationDate |
| Test Company | testaddress@direct.testcompanyaddress.com | CertificateInstalled | test address | 8/17/2016 | 8/17/2017 |
| Test Company | direct.testcompany.com | CertificateInstalled | Test User | 8/17/2016 | 8/17/2017 |

All fields in the CSV will be shown whenever a report is downloaded. These fields include:

- CompanyName
- Subject
- Status
- Representative
- DateRequested
- ExpirationDate

## AUDIT LOGS AND NOTIFICATIONS

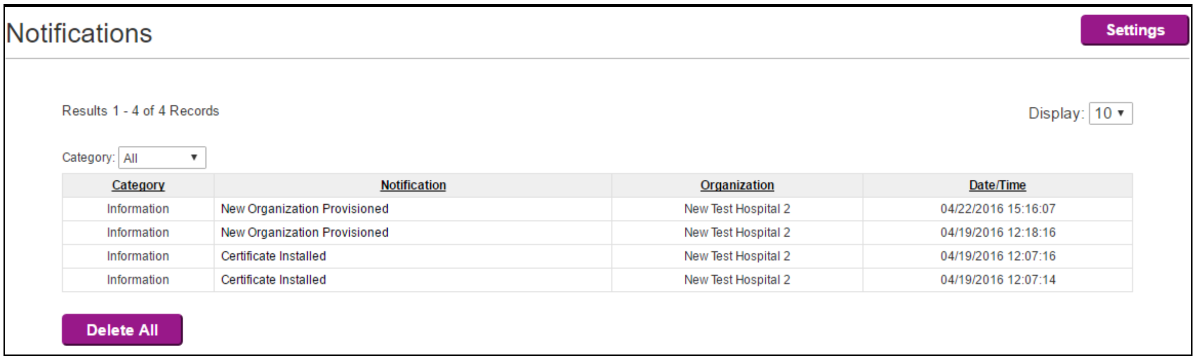
A set of audit logs will be available for the DataMotion Officer that is in charge of handling your overall account. These audit logs contain metrics that pertain to the various actions that can take place on the portal. While it is not possible for these logs to be accessed by anyone other than a DataMotion Officer, a subset of these logs will be generated on the Notifications page.

These notifications act as a method to keep track of all actions that take place on either the DPP itself, or on one of the messaging portals under the HCOs control. The types of notifications that will appear are for the following occurrences.

- Error
  - » These notifications always mean that something has failed either due to data input errors or to a validation error.
- Information
  - » Usually when these notifications appear it means that an action was successfully carried out.
- Warning

» Precautionary information that will state when certain things are close to expiration such as certificates and users, or when an action was not fully completed like creating a new HCO.

It is possible to select any one of the choices listed above, or all of them by using the **Category:** drop-down on the page.


Notifications
Settings

Results 1 - 4 of 4 Records

Display: 10

Category: All

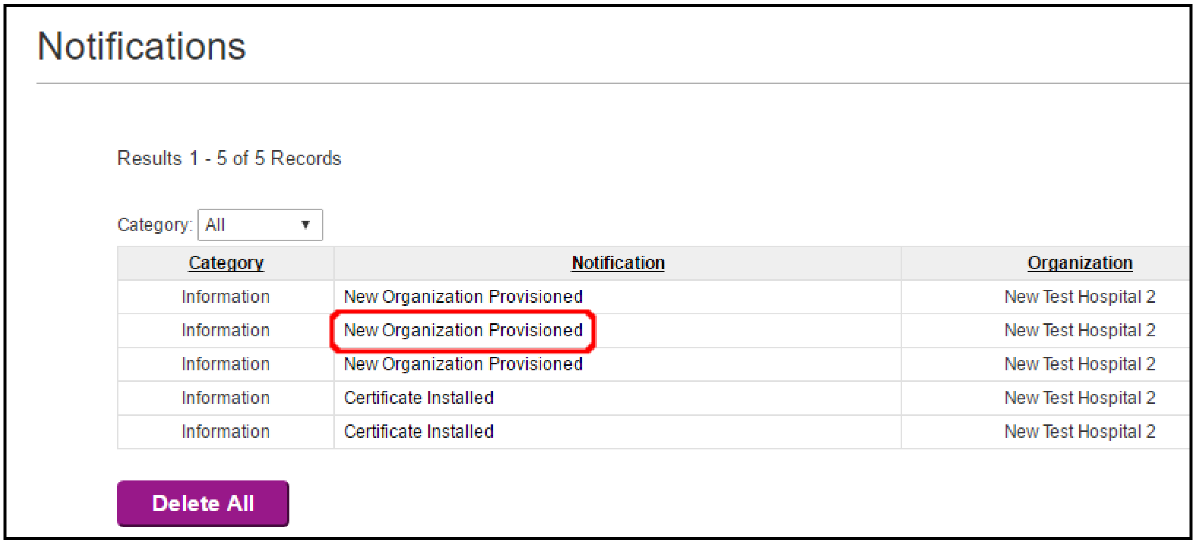
| Category | Notification | Organization | Date/Time |
|---|---|---|---|
| Information | New Organization Provisioned | New Test Hospital 2 | 04/22/2016 15:16:07 |
| Information | New Organization Provisioned | New Test Hospital 2 | 04/19/2016 12:18:16 |
| Information | Certificate Installed | New Test Hospital 2 | 04/19/2016 12:07:16 |
| Information | Certificate Installed | New Test Hospital 2 | 04/19/2016 12:07:14 |

Delete All

If the Notifications page gets too cluttered or if you decide that there is no longer any need to have the notifications that currently populate the table, you can select the Delete All button to remove.

**NOTE: It is not possible to delete a single notification or groups of notifications at a time.**

Some of the notifications will links that can be interacted with depending on the action that they link to. For example, if an Administrator creates a new company in the hierarchy, any other Administrator user type at the same hierarchical level can see that the company was created on the Notifications page and click the link to go directly to that company's Home page on the DPP. Clicking on the **New Organization Provisioned** link in this case would take the administrator directly to the organization that was provisioned. The following screens show the result of this example.




After clicking on the Notification the Admin will be brought to the new company.


* * *

This represents the end of the *DataMotion Direct Provisioning Portal Administration Guide*.