

Direct Messaging

Direct Messaging is a way for Providers and Patients to communicate that is both secure and standardized. While resembling email in many ways, Direct Messaging uses a very different standard than typical email. As a result, Providers and Patients must use Direct Addresses which are both unique and separate from their email.

It is important to note that Direct Messaging is only available to providers within a practice. This means that Staff users will be unable to communicate via Direct Messaging. This is due to the vetting process for Direct Messaging within a practice, which requires that a user possess a valid NPI to be provisioned with a Direct Address.

Contents

Direct Messaging Setup	2
Direct Domain.....	2
Direct Address.....	3
Provider Vetting.....	3
NPI Validation	4
Voice Validation and Confirmation Code	4
Personal Information.....	5
Credit Card Information.....	5
Validate.....	6

Direct Messaging Setup

Before a provider can send a Direct Message, there are several steps that need to be taken related to the configuration and setup of the Direct Messaging feature. First, the ADMIN user within the practice must configure the practice's Direct Domain. After the Direct Domain has been created, each provider within the practice must be configured with a Direct Address. Finally, once each provider that wishes to use Direct Messaging has a Direct Address, one provider in the practice must be vetted for the practice to be able to send Direct Messages.

Direct Domain

The Direct Domain acts much like the domain name of an email address. For example, emails sent from Google's Gmail service have an email address of username@gmail.com. The "gmail.com" part of the email address is the domain name. Direct messages sent from Valant have a custom Direct Domain for each practice. The general format of Direct Addresses in Valant follow the pattern of: username@DirectDomain.valantdirect.com.

The Direct Domain can be configured by logging into the ADMIN area of the practice and navigating to **Persons and Institutions | Practice | Direct**.

Under the Direct tab, the Direct Domain can be set for the practice. The Direct Domain can be just about anything that the practice wants to use providing that the domain hasn't already been selected by another practice using Valant. Once the Direct Domain has been entered, clicking on the setup button will attempt to provision the domain.

It is important to note that once the domain has been set, it is permanently attached to that practice. Thus, care should be taken to ensure that the Direct Domain is properly spelled and matches the practice in question.

The Vetted Status will indicate false until at least one provider within the practice has been vetted. Once a practice has their Direct Domain entered and the setup is successful, the domain will display under the Direct tab. This is what will appear to the right of the '@' symbol in the provider's Direct Address. In the example shown below, a Direct Message sent from this practice would appear as: username@mu2014.valantdirect.com.

Direct Messaging has been setup and is ready to be used.

Direct Domain: mu2014.direct.updoxqa.com
Vetted Status: True

Direct Address

After a practice has been set up with a Direct Domain, the providers within the practice can now be configured with a Direct Address. The Direct Address is the 'username' part of username@DirectDomain.valantdirect.com.

Each provider that wishes to make use of Direct Messaging must first be configured with a Direct Address. This can be done by logging into the ADMIN area of the practice and navigating to **Persons and Institutions | Providers | Direct**.

If the provider has not yet been configured with a Direct Address, then the ADMIN can provision one by entering the username in the box provided and clicking the **Setup** button. The username can be just about anything that the provider wants to use assuming that the username hasn't already been selected by another provider within the practice.

It is important to note that once the username has been set, it is permanently attached to that provider. Thus, care should be taken to ensure that the username is properly spelled and matches the provider in question.

Once a provider has been configured with a Direct Address, the Direct tab will display the completed Direct Address for the provider. An example of a Direct Message address is: jamesgetwell@mu2014.valantdirect.com.

Provider Vetting

Once the provider has a Direct Address, the practice needs to be vetted before any Direct Messages can be sent. Any provider within the practice can be vetted. Once a single provider has been vetted, then the entire practice is considered vetted and all providers within the practice can send Direct Messages. The vetting process begins by clicking **Vet as this User** in **Persons and Institutions | Providers | Direct**.

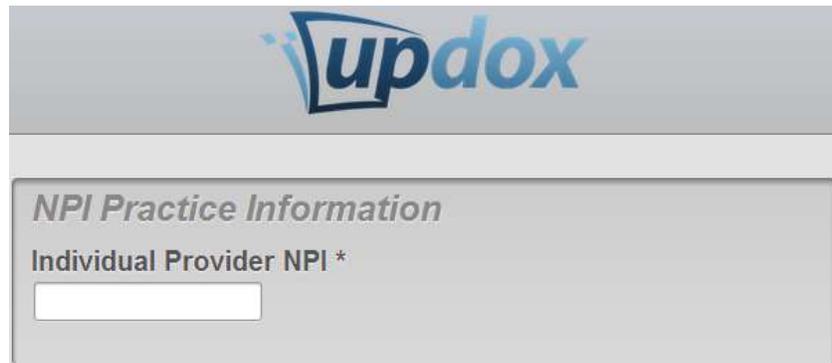
The vetting process consists of four steps:

1. NPI Validation
2. Voice Validation and Confirmation Code
3. Personal Information
4. Credit Card Verification.

All four steps need to be completed in order for a provider to be considered vetted. Fortunately, only a single provider needs to be vetted for the entire practice to be considered vetted. Even if that provider leaves the practice, the practice will still be considered vetted so long as the Direct Address associated with the vetted provider is not made inactive.

NPI Validation

The vetting for providers related to Direct Messaging is handled by our partner Updox. The first step in the vetting process is to enter the NPI number of the provider being vetted.



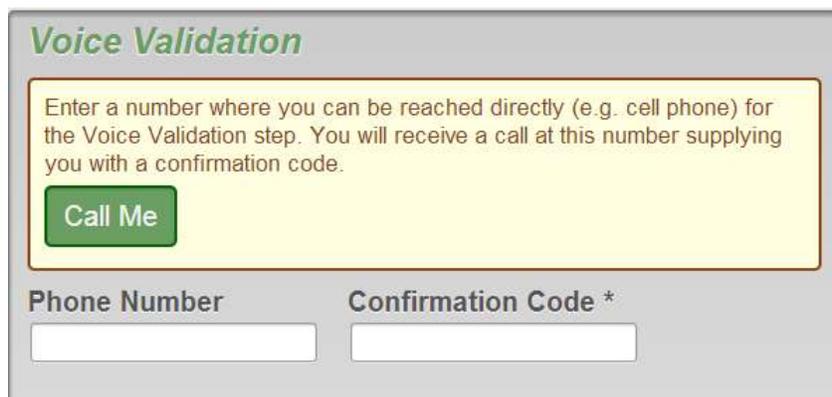
The screenshot shows the Updox logo at the top. Below it, the heading "NPI Practice Information" is displayed. Underneath, the label "Individual Provider NPI *" is followed by a single-line text input field.

Once the NPI number is entered, the provider's information tied to the NPI will be displayed. The data is pulled from the National Plan & Provider Enumeration System (NPPES) website and is refreshed each week by Updox. It is important that the information displayed is accurate for the vetting process to continue. If the information shown is incorrect, the provider must contact NPPES to update the data connected to their NPI number.

Voice Validation and Confirmation Code

After the NPI has been entered for the provider and the information associated with that NPI has been verified, the next step is for the provider to receive a Confirmation Code from Updox. To receive the code, a phone number must be entered in the space provided and the **Call Me** button clicked. Once the Call Me button is clicked, an automated service by Updox will call the provider using the number entered. The provider will verify their identity and be given the Confirmation Code. The code should then be entered in the Confirmation Code field.

The phone number provided needs to be answered by the provider being vetted. In addition to receiving the Confirmation Code, the provider must confirm their identify with Updox.



The screenshot shows a form titled "Voice Validation". Inside a yellow-bordered box, there is a text instruction: "Enter a number where you can be reached directly (e.g. cell phone) for the Voice Validation step. You will receive a call at this number supplying you with a confirmation code." Below this instruction is a green "Call Me" button. At the bottom of the form, there are two input fields: "Phone Number" and "Confirmation Code *".

Personal Information

Once the Confirmation Code has been entered, the next step is to enter the personal information for the provider being vetted. The First Name, Last Name, Date of Birth, and Phone Number of the provider all need to be entered and must match the information associated with the credit card used in the next step. Also, the provider's email address must also be submitted. The Email Address is used by Updox for support purposes only and does not need to match the information tied to the NPI for this provider.

Credit Card Information

The final bit of information required for a provider to be vetted is their Credit Card Number and Credit Card Billing Address. This information is used solely for identification purposes and no charges will be levied.

Updox uses Equifax for their validation. A provider must have a credit card whose information is contained within Equifax in order to make use of this verification process. The data entered for the credit card number and address must match the information contained within Equifax. Three failed attempts will lock out this provider and Updox will need to be contacted in order to restart the verification process.

If a provider does not have a credit card or their credit card is not shared with Equifax, then a video conference must be set up with Updox. The provider will need to be able to show Updox a picture of their driver's license during the video conference in order for them to be verified.

The credit card used for vetting the provider must be the personal credit card of the provider and not a credit card associated with the practice. The credit card is used for verification purposes only and will not be stored or charged by Updox.

Personal Credit Card Information

For this identity verification you must:

- Use a personal credit card
- Enter the name as shown on the card and the billing address
- Do not use a credit card for the practice

Don't worry; there is no fee, it does not count against your credit score, and we do not keep the information.

Credit Card Number*

Credit Card Billing Address*

Validate

Once all of the steps listed above have been completed, the final action required in order to vet a provider is to check the checkbox labeled “I certify this practice is HIPAA compliant” and click the Validate button. Doing so will attempt to verify the following three items for the provider:

1. Identity (personal info and credit card)
2. Account (NPI)
3. Voice (Confirmation Code).

All three of these items need to be verified in order to complete the vetting process.

Validation was unable to successfully confirm provided information.

Identity Verification	NOT VERIFIED
Account Verification	NOT VERIFIED
Voice Verification	NOT VERIFIED

I certify this practice is HIPAA compliant.

[Validate](#)

* Fields are required for validation
Use of trademarked names for subdomain submission not owned by the person registering is strictly prohibited.

[Get Help](#) 

Once a provider has been vetted in a practice, both the Direct tab under **Persons and Institutions | Practice** and under **Persons and Institutions | Provider** will indicate that the Vetted Status is **True**.