User Guide

ForwardHealth Provider Portal Account

July 15, 2024

WISCONSIN DEPARTMENT of HEALTH SERVICES

Table of Contents

1 Introduction

The ForwardHealth Portal allows providers to conduct business through a secure entry point 24 hours a day, seven days a week. After creating a secure Provider Portal account, providers can perform various functions including verifying member enrollment; submitting electronic claims, adjustments, and prior authorization requests; and viewing other reports and data. To avoid a delay in service, providers must provide contacts and communicate in a timely manner.

2 Request Portal Access

To establish a Provider Portal account, providers will need a PIN. Providers can establish as many provider Portal accounts as needed for their business. Helpdesk support information is available in the Appendix: Portal Helpdesk Support of this guide.

1. To request a PIN, access the Portal at https://www.forwardhealth.wi.gov/.

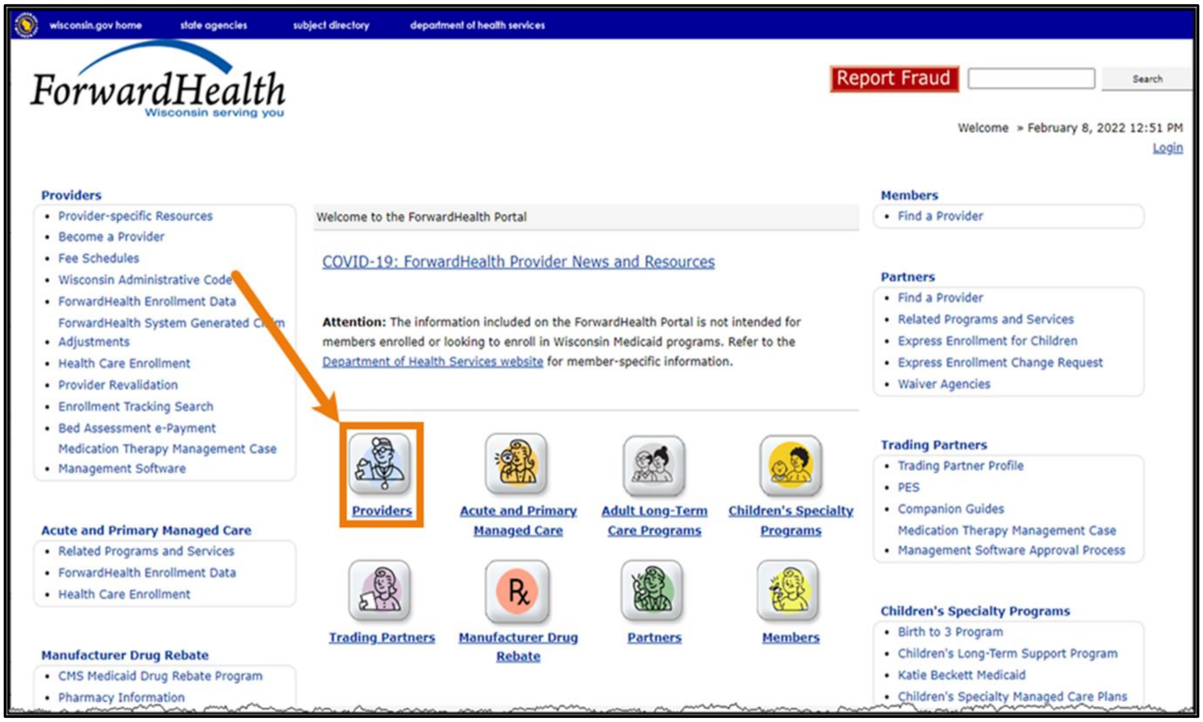


Figure 1 ForwardHealth Portal Homepage

2. Click **Providers**. The public page for the Provider area of the Portal will be displayed.

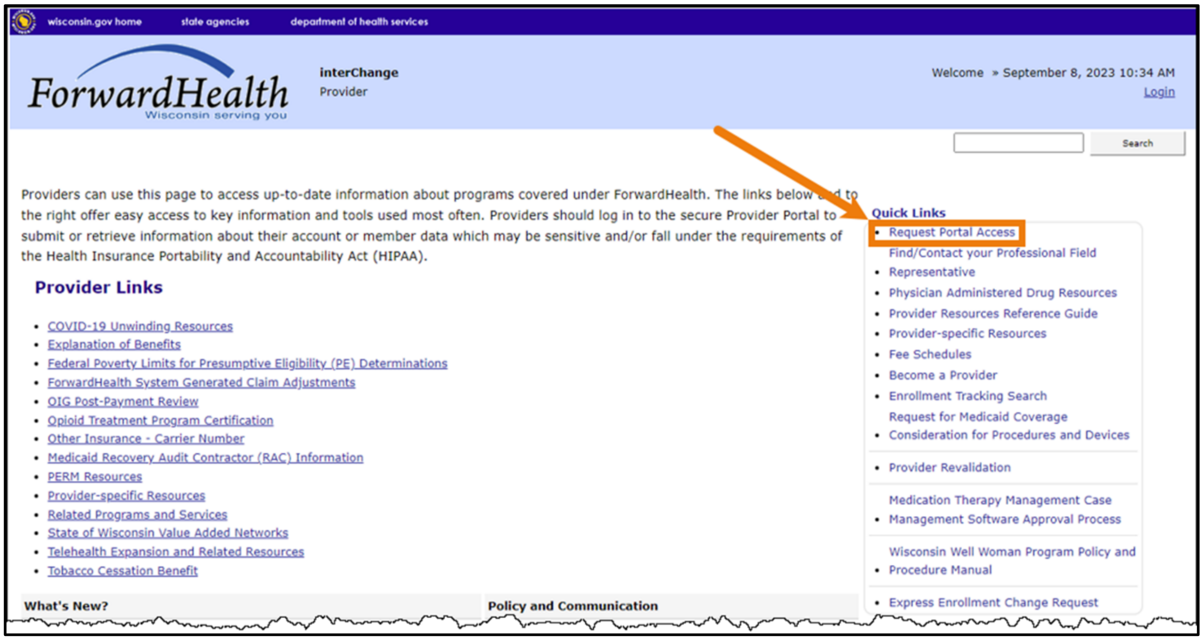


Figure 2 Public Provider Page

3. In the Quick Links box on the right of the page, click **Request Portal Access**. The Request Portal Access page will be displayed.

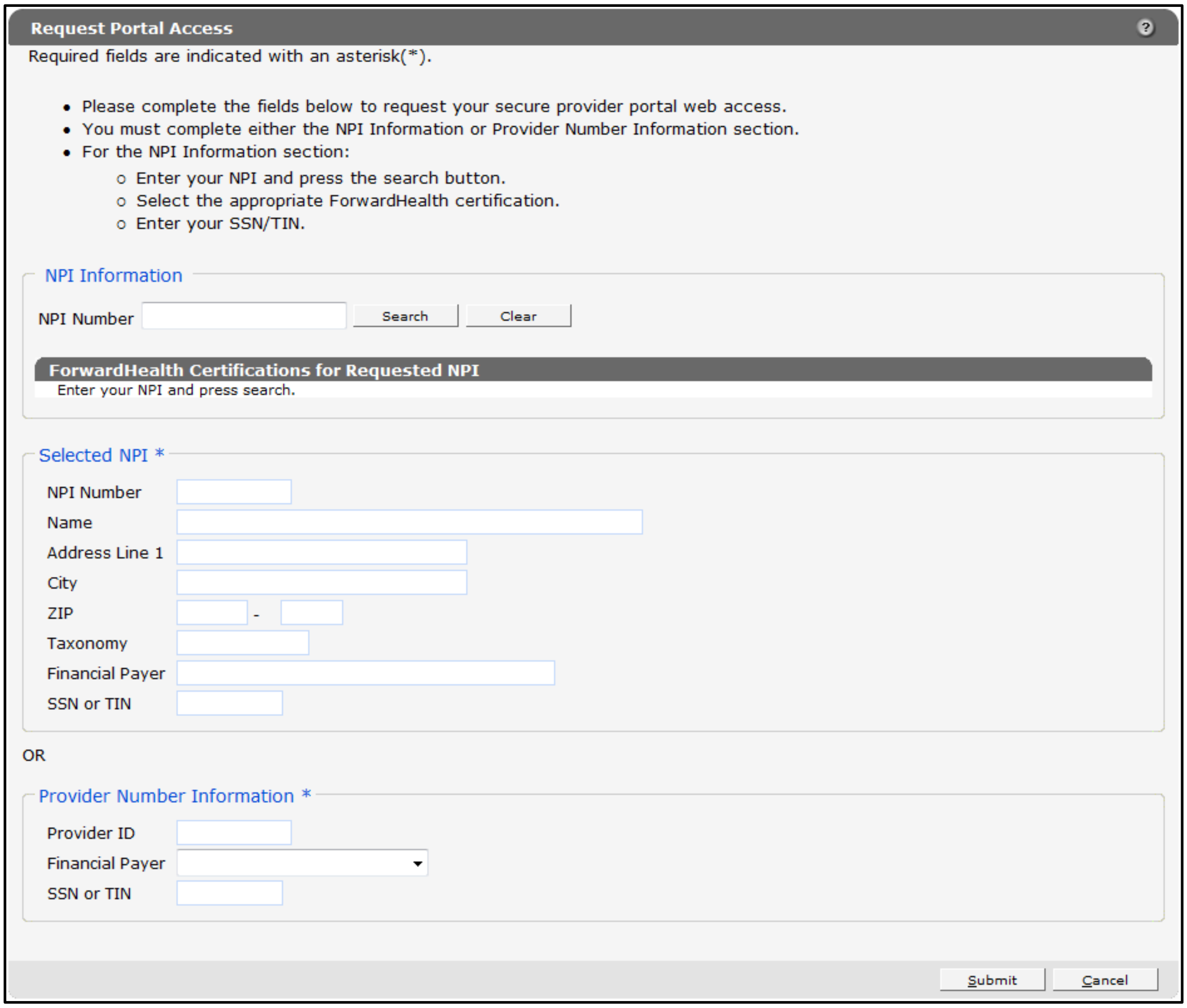


Figure 3 Request Portal Access Page

4. In the "NPI Information" section, enter the provider's National Provider Identifier (NPI) in the NPI Number field if the user is a health care provider.

   If the user is not a health care provider (for example, a personal care only provider, a specialized medical vehicle provider, or a blood bank), they can proceed to Step 9 of this guide.

5. Click **Search**.

   The "ForwardHealth Certifications for Requested NPI" section will auto-populate with the provider's information that ForwardHealth has on file.

   If the NPI is not found, the page will refresh; however, the "ForwardHealth Certification for Requested NPI" section will not be populated with the provider's information.

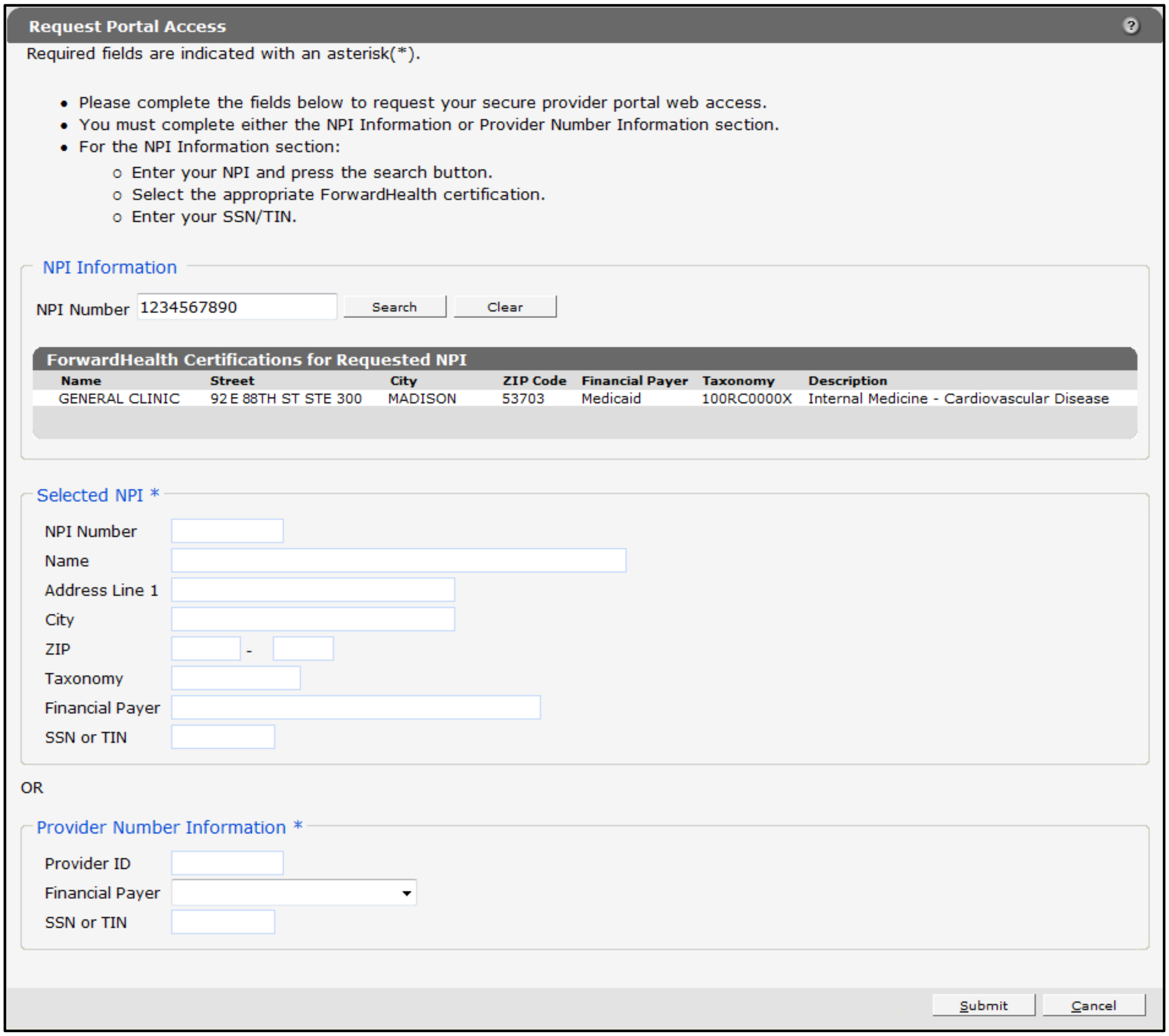


Figure 4 Request Portal Access Page

6. Click the appropriate row from the "ForwardHealth Certifications for Requested NPI" section. The "Selected NPI" section will auto-populate with the selected information.

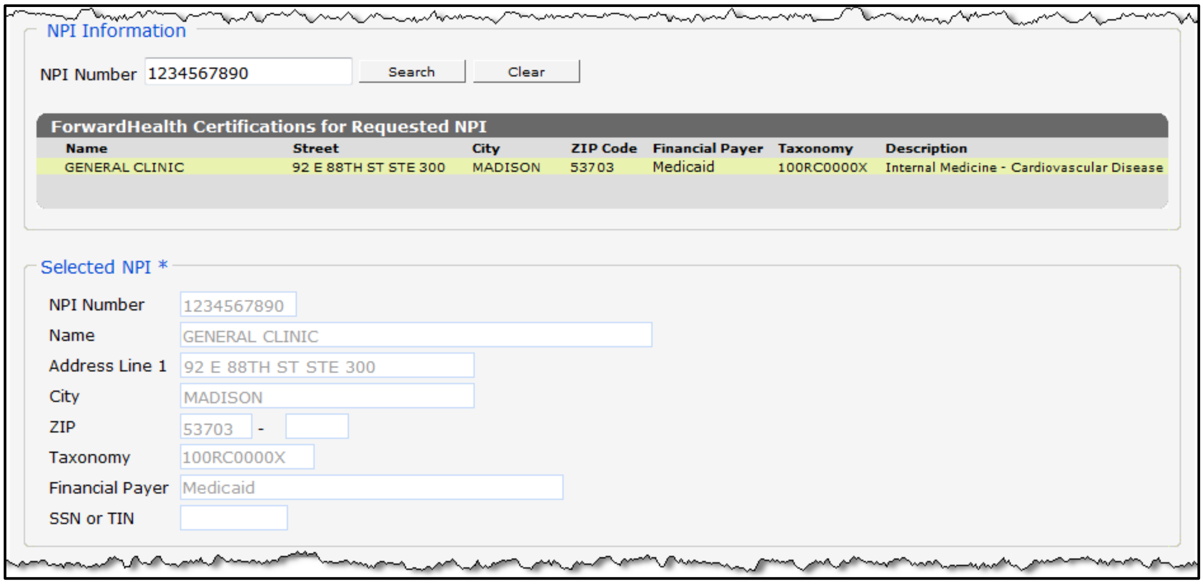


Figure 5 Selected NPI Section With Auto-Populated Information

7. Enter the provider's Social Security number (SSN) or Tax ID Number (TIN) in the SSN or TIN field in the "Selected NPI" section.

8. Skip to Step 12 of this guide.

9. If the provider is not a health care provider and therefore does not have an NPI, enter the provider's Medicaid Provider ID in the "Provider Number Information" section.

10. From the Financial Payer drop-down menu, select the financial payer certification for which the provider is requesting a Provider Portal account.

11. Enter the provider's SSN or TIN in the SSN or TIN field.

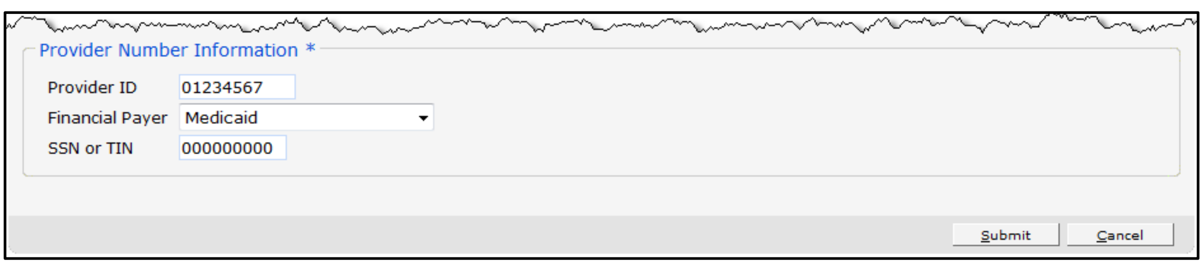


Figure 6 Provider Number Information Section

12. Click **Submit**. If the request is successful, a confirmation page will be displayed.

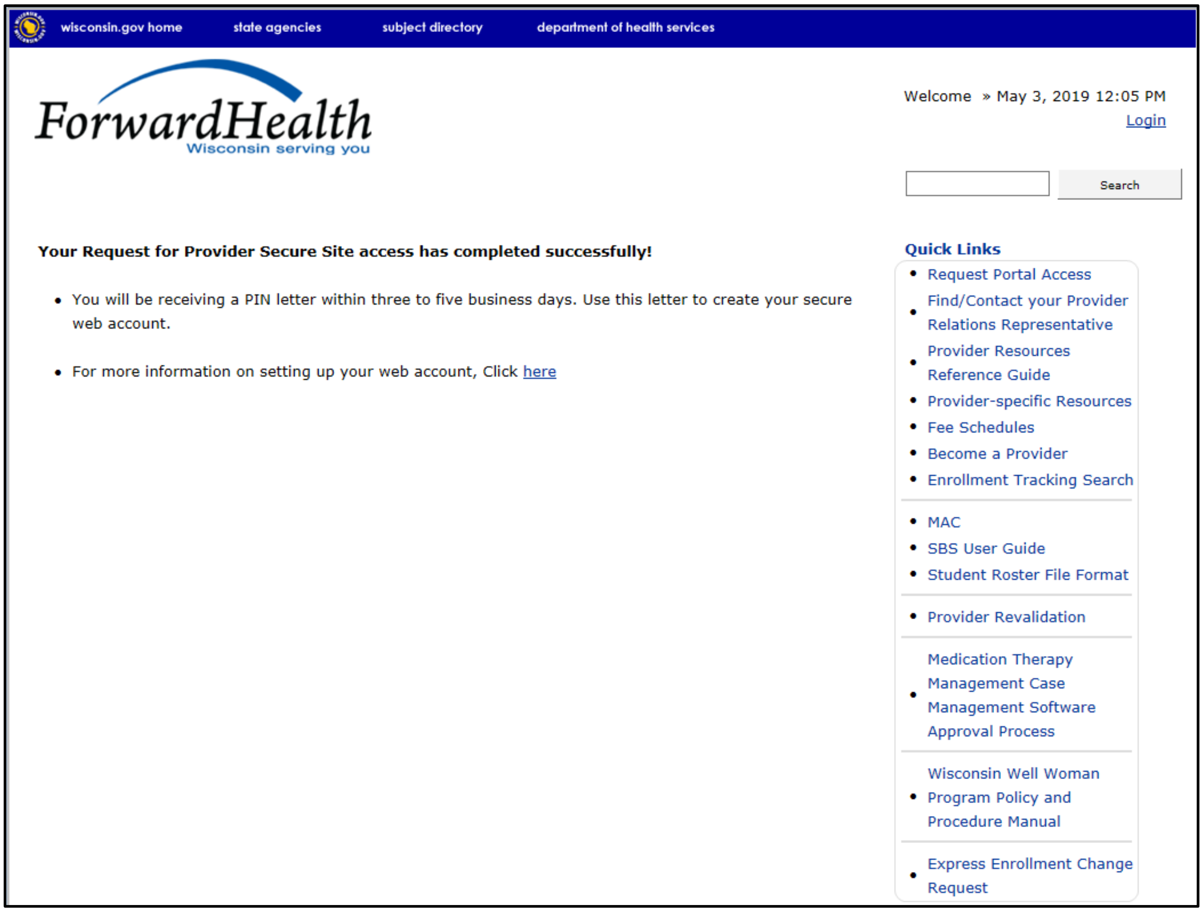


Figure 7 Confirmation Page

If the request is not successful, an error message indicating why the information could not be submitted will be displayed at the top of the page.

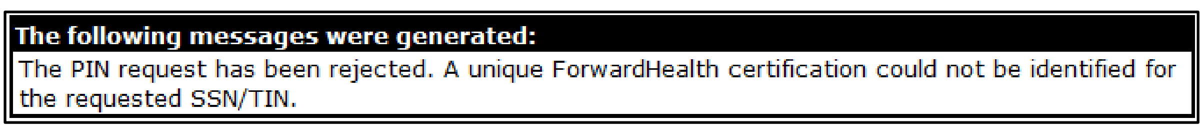


Figure 8 Example Error Message

A request could be denied for some of the following reasons:

- No provider agreement on file. Call Provider Services at 800-947-9627 for the agreement.
- The SSN or TIN number is incorrect. Verify the number and enter the correct number.
- A PIN was already requested. Check within the organization to find out if someone has already received the PIN and set up an account(s).

If the user has questions, they may call the Portal Help Desk (toll free) at 866-908-1363 Monday through Friday between 8:30 a.m. and 4:30 p.m.

After a provider has successfully requested Portal access, a letter containing a PIN will be mailed to the provider. Access to the Portal is **not** possible without a PIN. The letter also includes a Login ID, which is a health care provider's NPI or a non-health care provider's Medicaid Provider ID. For security purposes, the Login ID contains only the third through sixth digits of the NPI or Provider ID.

Tony Evers
Governor

Karen E. Timberlake
Secretary

State of Wisconsin
Department of Health Services

FORWARDHEALTH

ELECTRONIC DATA INTERCHANGE UNIT
313 BLETTNER BLVD
MADISON WI 53784

Telephone: 866-416-4979
Fax: 608-221-0885
TTY: 711
www.dhs.wisconsin.gov/forwardhealth

Month X, 20XX

Im A. Provider
XYZ Clinic
123 Main St
Anytown WI 55555-1111

Dear Provider:

ForwardHealth has received your request to establish a secure Portal account. A summary of the information you provided is included below, along with a Login ID and Personal Identification Number (PIN) you will need in order to set up your secure provider account on the ForwardHealth Portal.

NPI or Provider ID:	xx3456xxxx
Provider Type/Specialty:	Physician/Internal Medicine
Taxonomy:	XXXXXXXXXX
Zip Code:	55555-1111
Financial Payer:	Medicaid

Please note that for security purposes, only digits 3, 4, 5, and 6 of your NPI or Provider ID are shown.

To create your secure Provider account:

- Go to the ForwardHealth Portal at *www.forwardhealth.wi.gov/*.
- Select the "Providers" button.
- Select the Logging in for the first time? link under "Login to Secure Site".
- Enter your Login ID and PIN:
  Login ID: XXXXXXXXXX
  PIN: XXXXXXXXX

Detailed instructions and helpful hints on setting up your secure provider account can be found at *www.forwardhealth.wi.gov/*.

Sincerely,

<Department Name>

F-13512 (10/08)

www.dhs.wisconsin.gov

Figure 9 PIN Letter

3 Set Up an Account

After receiving a PIN letter, administrative account users may set up an account on the Portal. Users will use the Login ID and PIN from the PIN letter to create a user name and password as well as to enter contact and security information.

For information about adding a new organization to a current account, refer to Chapter 9 Add Organization of this guide.

3.1 Account Types

Three different account types are available through the Portal. Access to certain features or functions on the Portal is determined by the account type assigned to the user. Through these different account types, a high level of security and accountability is maintained:

- *Administrative accounts*—The user who establishes the Portal account with the Login ID and PIN (from the PIN letter) is considered the account administrator and is responsible for managing the Portal account. Administrative accounts are granted complete access to all functions and applications within the Provider area of the Portal and have the ability to add, remove, and manage other account types and their access. The account administrator is responsible for performing regular reviews of clerk accounts to ensure they are up to date.

  Each service location (certification/provider file) can only have one user designated as an account administrator; however, multiple service locations can be attached to the same account administrator.

- *Clerk accounts*—Administrative accounts can set up clerk accounts with access to any or all of the roles available to the administrative account. If a new role becomes available, that role may be assigned to a clerk account. A clerk account can be added to multiple organizations to allow one clerk access to multiple organizations.

- *Clerk administrative accounts*—Clerk accounts may be granted clerk administrative rights. A clerk administrative account can create new clerk accounts with access to any or all of the roles to which the clerk administrative account has access and can delete and manage clerk accounts under their purview.

3.2 Logging in for First Time

After the administrative account user receives the PIN letter, they can access the Portal at https://www.forwardhealth.wi.gov/.

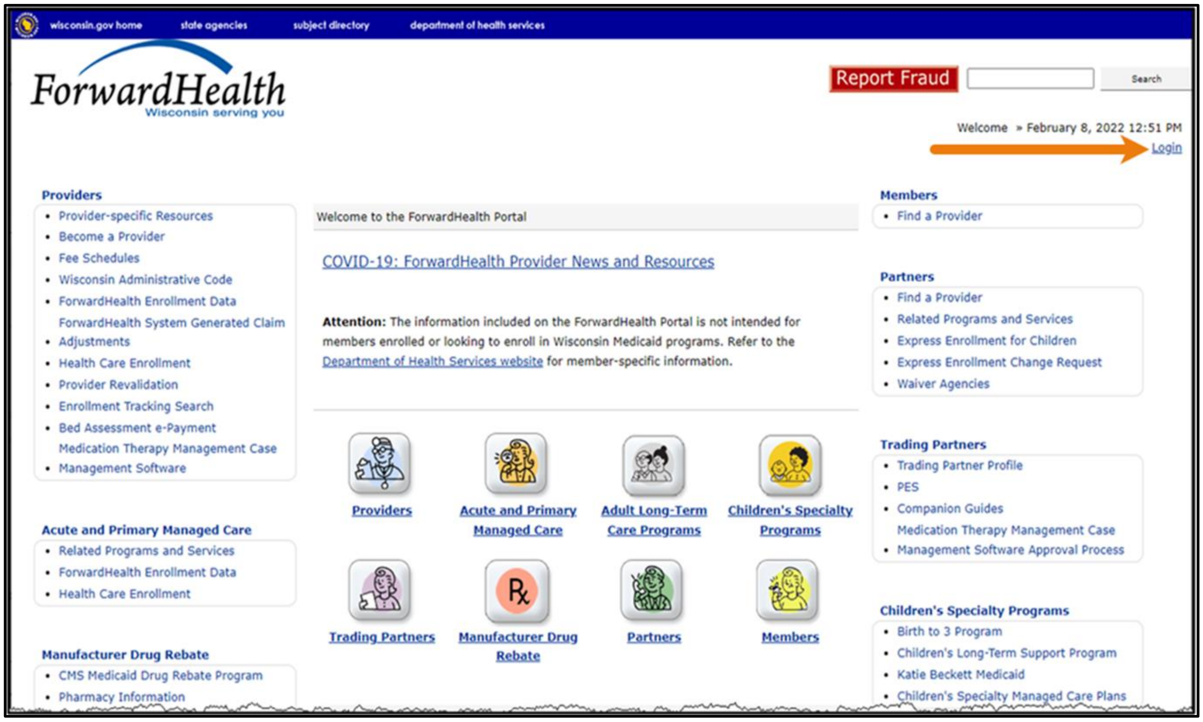


Figure 10 ForwardHealth Portal Homepage

1. Click **Login**. A Sign In box will be displayed.

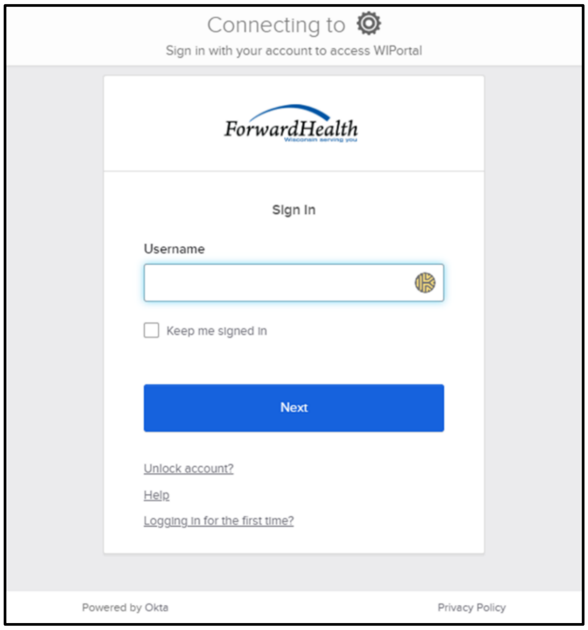


Figure 11 Sign-In Box

2. Click **Logging in for the first time?**

The Account Setup page will be displayed.

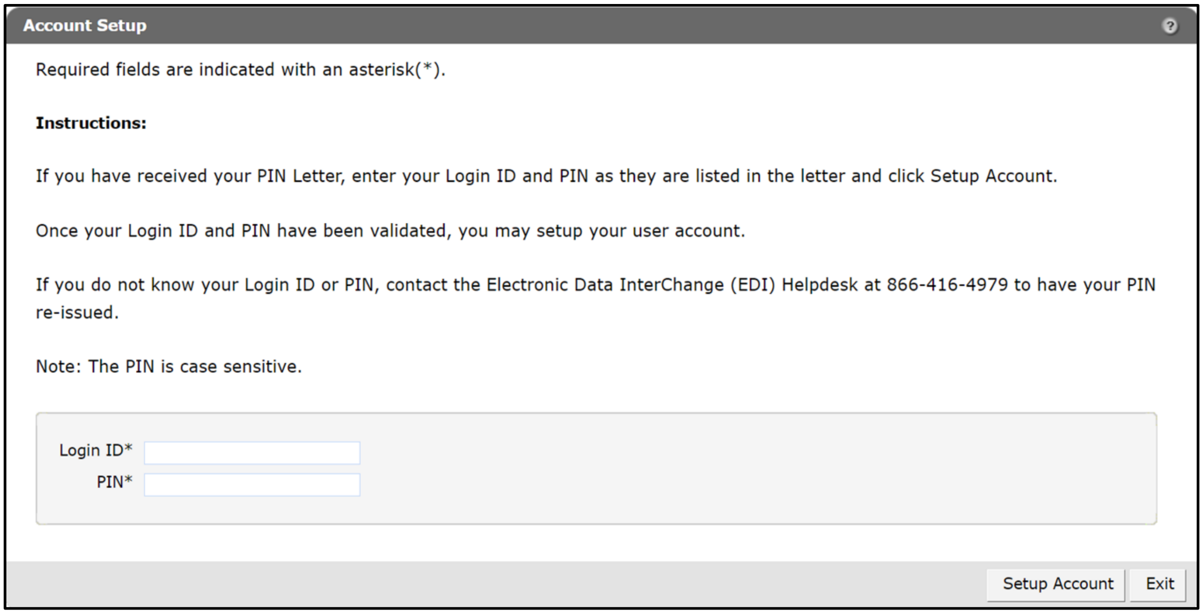


Figure 12 Account Setup Page

3. Enter the Login ID and PIN listed in the user's PIN letter.

   For security purposes, the PIN letter will contain only four digits of the NPI or Medicaid Provider ID reported; however, users should **enter the entire** NPI or Medicaid Provider ID in the Login ID field.

   The PIN from the PIN letter can only be used once. After the account has been established, the PIN cannot be used again.

4. Click **Setup Account**. The Administrator setup page will be displayed. Note: When new provider administrators create a Portal account, they are required to provide backup contact information during account setup. Provider administrators will not be able to use the same contact information for both the administrator account and the backup contact. Refer to Chapter 7 Administrator Backup Information of this guide.

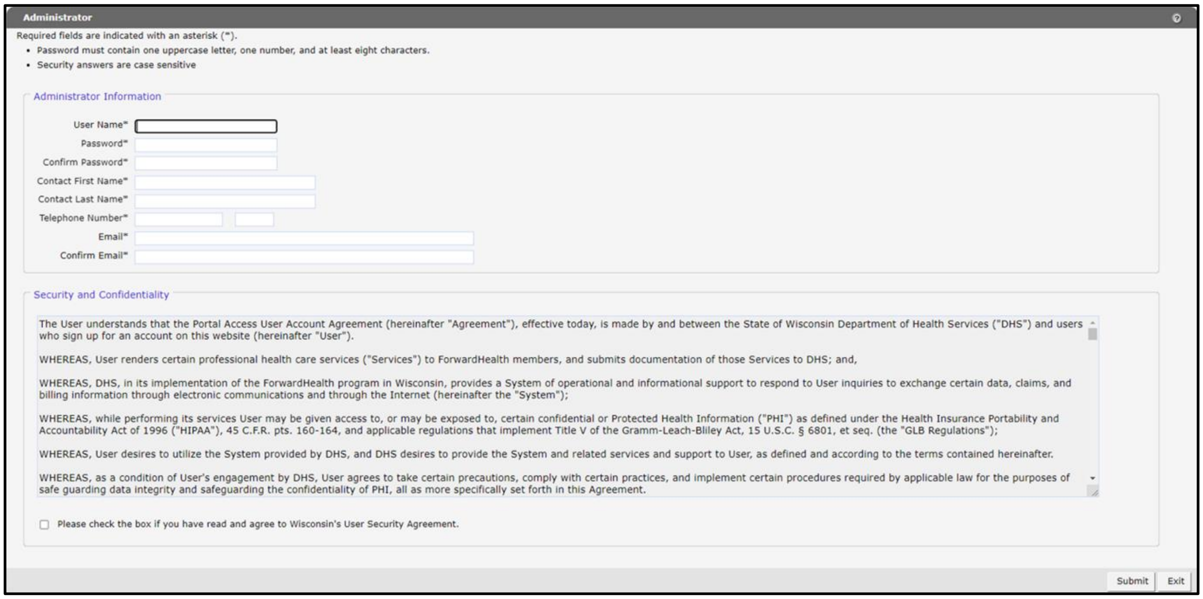


Figure 13 Administrator User Profile Page

5. Enter information in the fields. It is necessary to **complete all the fields** on this page.

   - The user name must be between six–20 characters and can only contain letters and numbers. The user name is not case-sensitive.

     Note: The user name cannot be changed without deactivating the account.

   - The password must be between nine–15 characters and must contain three different types of characters such as uppercase letters, lowercase letters, special characters, or numbers. The password must be unique and cannot contain information from the user name, contact first name, or contact last name.

   - The phone number must include the area code. The number will be auto-formatted.

6. Read the Security and Confidentiality agreement.

7. Check the agreement checkbox.

8. Click **Submit**. If the user receives an error message, correct the error(s) and click **Submit** again.

The License for Use of Physicians' Current Procedural Terminology, Fourth Edition (CPT) and Point and Click License for Use of Current Dental Terminology (CDT) agreements page will be displayed.

Figure 14 End User Point-and-Click License Agreements

9. Click the radio button next to "I Accept." Click **Submit Agreement**.

   Note: If "I Do Not Accept" is selected, the user will be returned to the Portal homepage and will not be able to access the secure Provider Portal.

10. The user's secure Provider page will be displayed.

Figure 15 Secure Provider Page

3.3 Reset Password

1. Access the Portal at https://www.forwardhealth.wi.gov/.
2. Click **Login**. A Sign In box will be displayed.

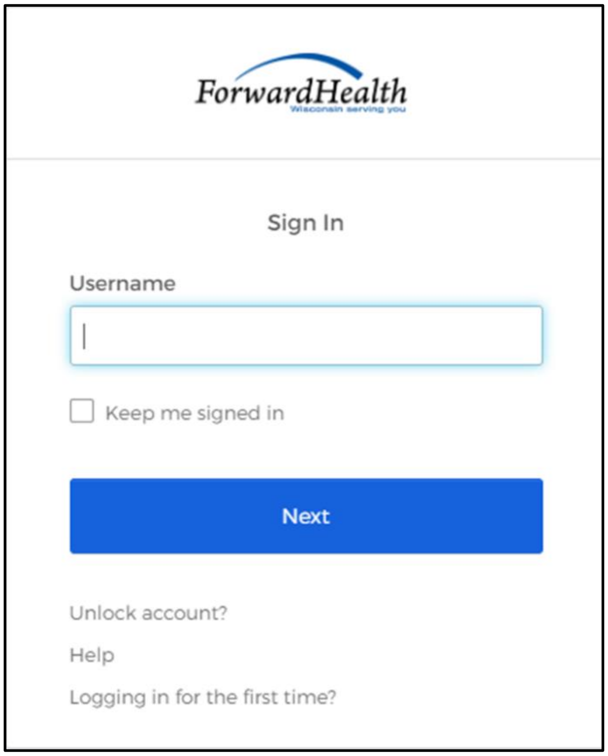


Figure 16 Sign In Box

3. Enter the user's username.
4. Click **Next**.

A Verify with your password box will be displayed.

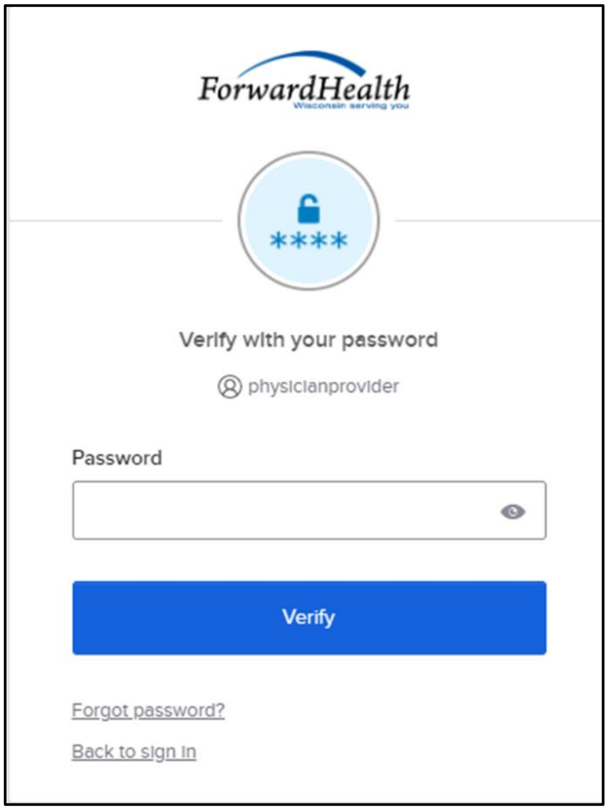


Figure 17 Verify With Your Password Box

5. Click **Forgot password?**

A Reset your password box will be displayed.

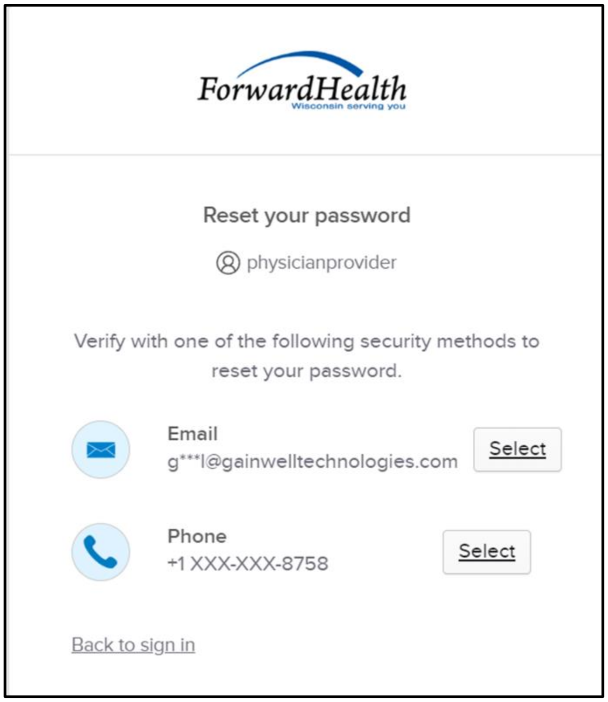


Figure 18 Reset Your Password Box

6. Click **Select** to receive a verification via email or phone.

- If the user clicks **Select** for email:

  a. A Get a verification email box will be displayed.

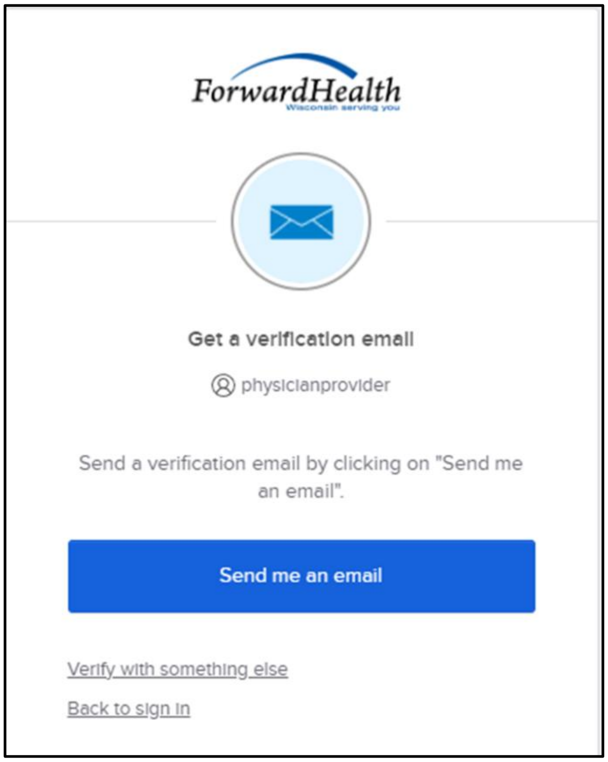


Figure 19 Get A Verification Email

  b. Click **Send me an email**. Note: The user also has the option to select **Verify with something else** which will take them back to the Unlock account box or **Back to sign in** which will take them back to the sign in page.

A verify with your email box will be displayed and an email will be sent.

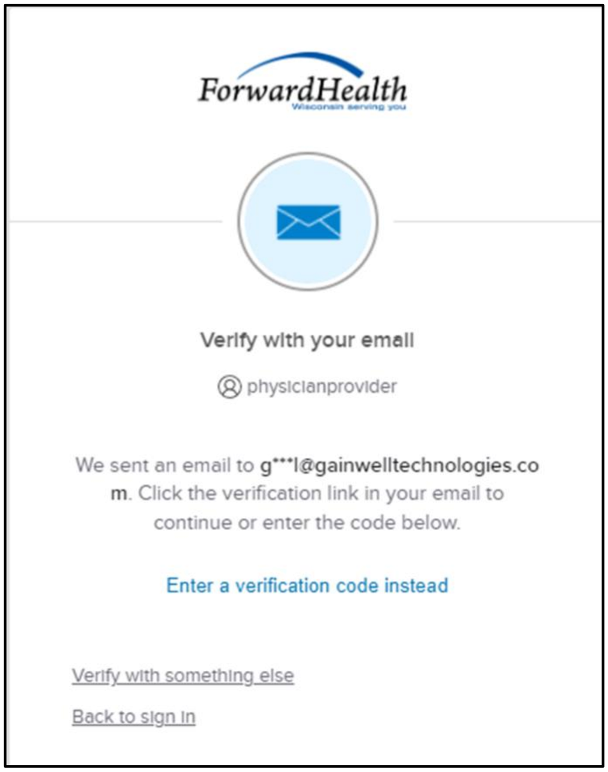


Figure 20 Verify With Your Email Box

c. Proceed to Step 7.

- If the user clicks **Select** for phone:

  a. A verify with your phone box will be displayed.

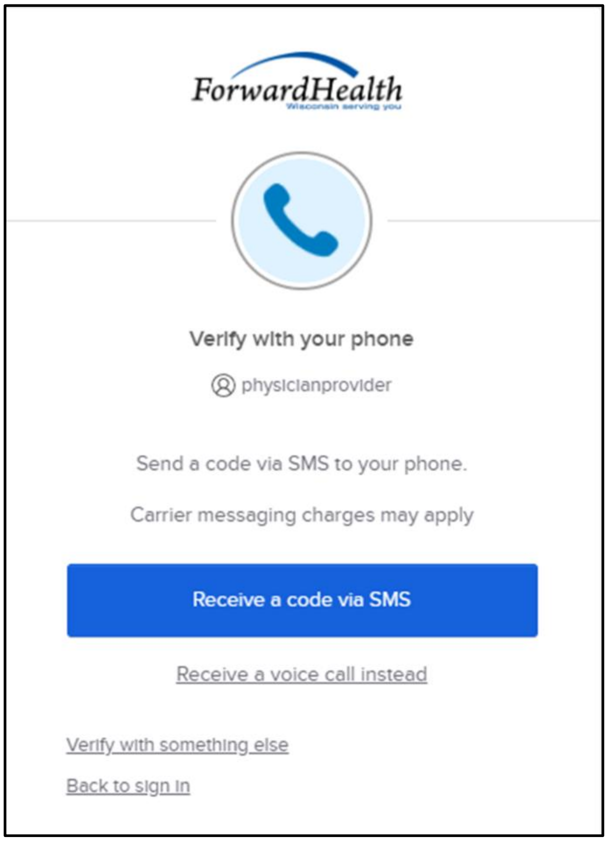


Figure 21 Verify With Your Phone Box

  b. Click **Receive a code via SMS** (text) or **Receive a voice call instead**. Note: The user also has the option to select **Verify with something else**, which will take them back to the Unlock account box, or **Back to sign in**, which will take them back to the sign in page.

A Verify with your phone box will be displayed.

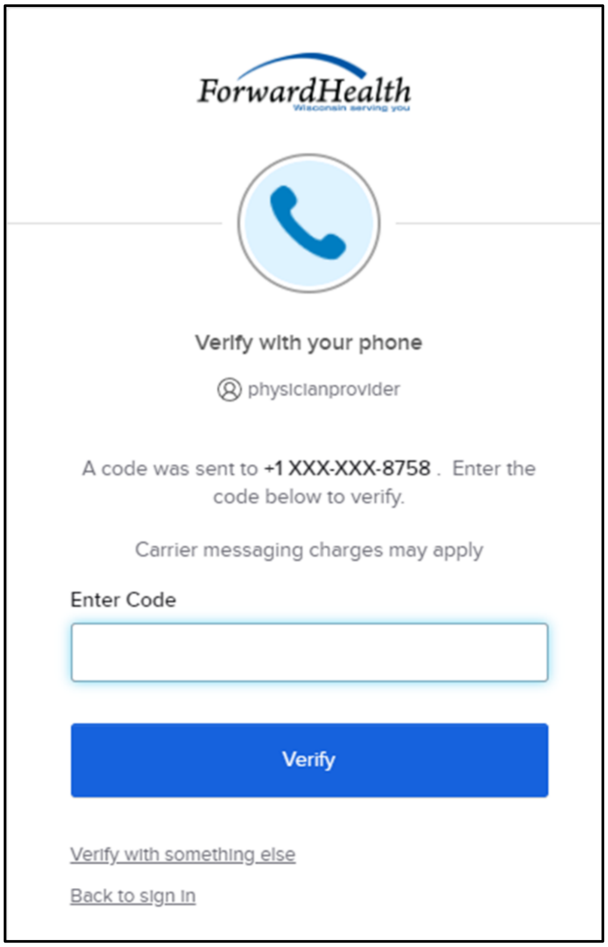


Figure 22 Verify With Your Phone Box

c. Enter the code that was sent.

d. Click **Verify**.

A Get a verification email box will be displayed.

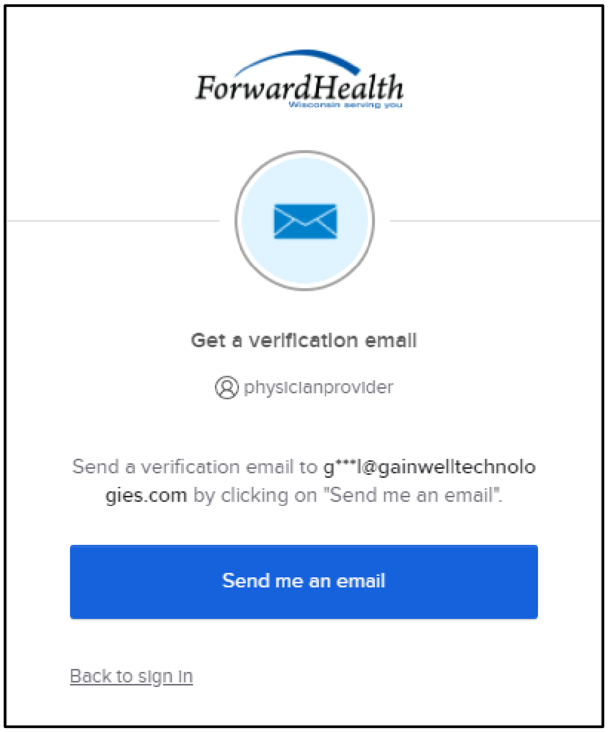


Figure 23 Get A Verification Email Box

e. Click **Send me an email**.

A Verify with your email box will be displayed and an email will be sent.

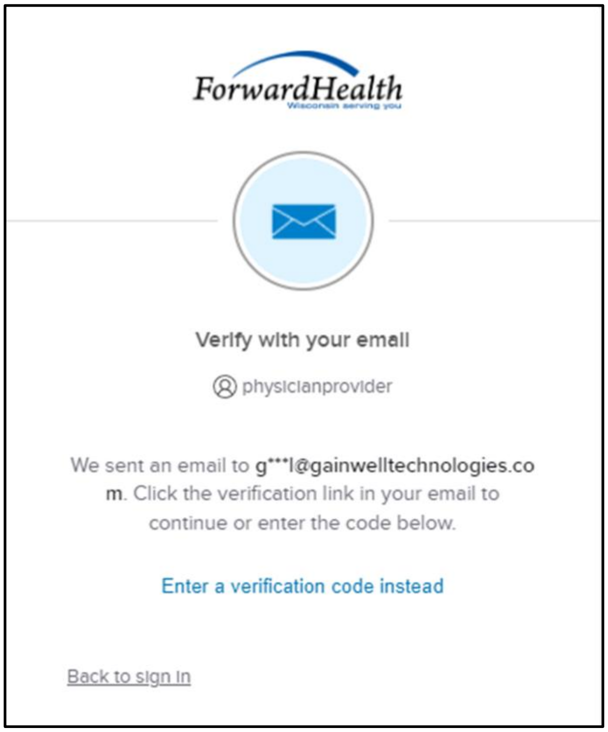


Figure 24 Verify With Your Email Box

7. The email sent to the user's email address includes a **Reset Password** link (Option 1) and a verification code (Option 2).

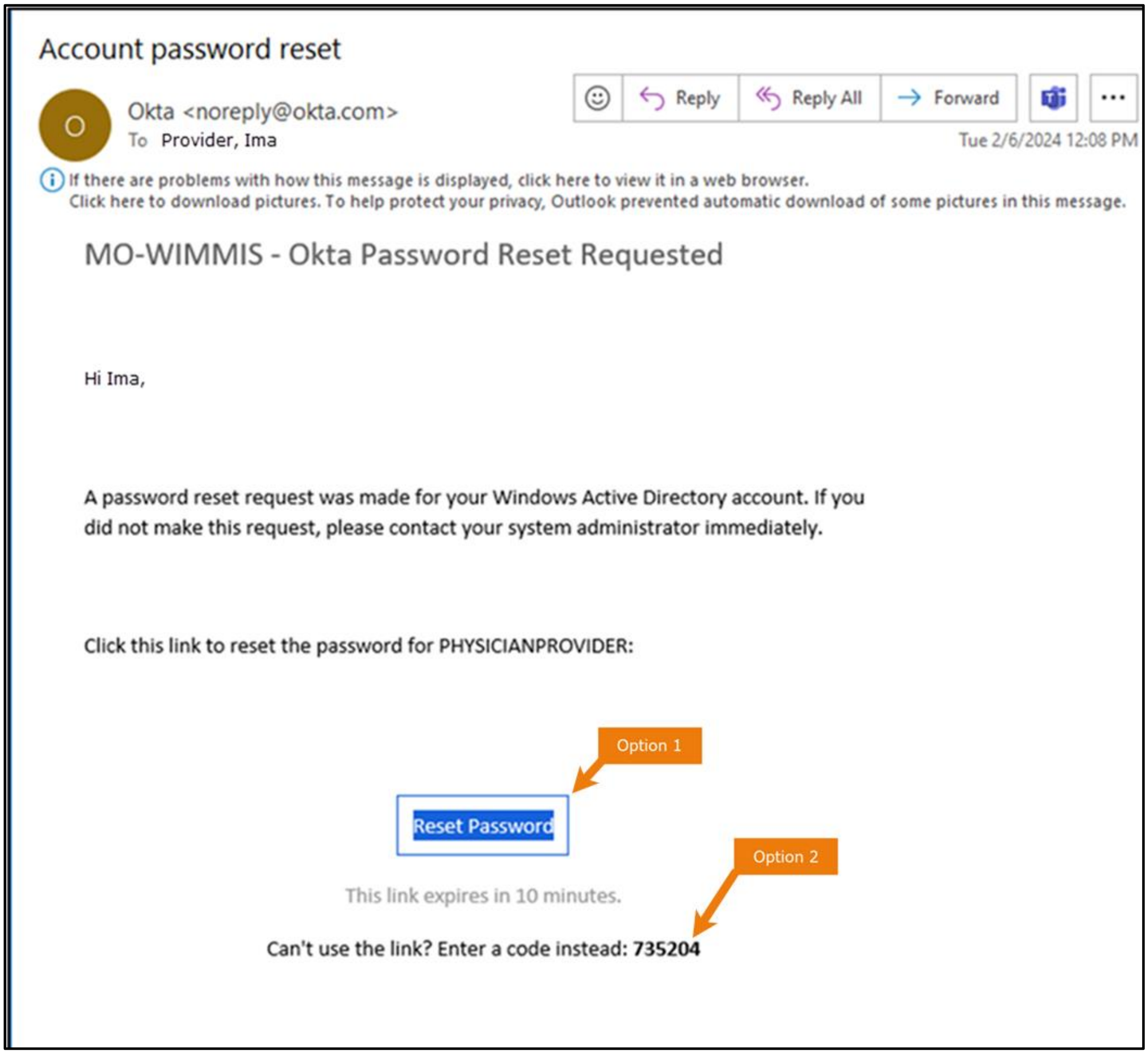


Figure 25 Account Password Reset Email

8. The user can choose to either click the **Reset Password** link (Option 1) or enter the verification code from the email (Option 2) instead.

- Clicking the **Reset Password** link from the email will display a verification code box.

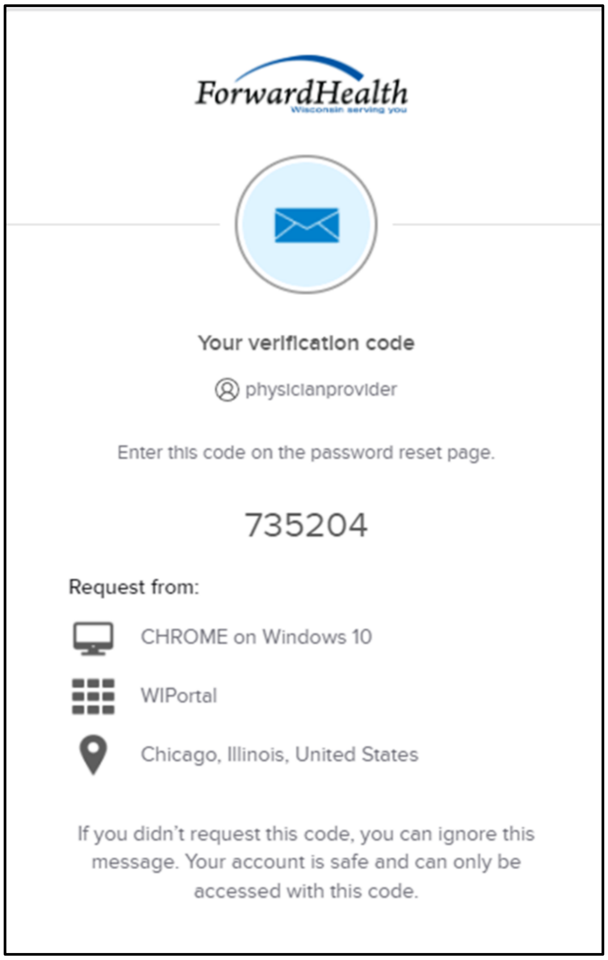


Figure 26 Verification Code Box

9. Copy the verification code from the verification code box or from the account password reset email, return to the verify with your email box, and click **Enter a verification code instead**.

10. Enter the code from the verification code box or the code from the account password reset email and click **Verify**.

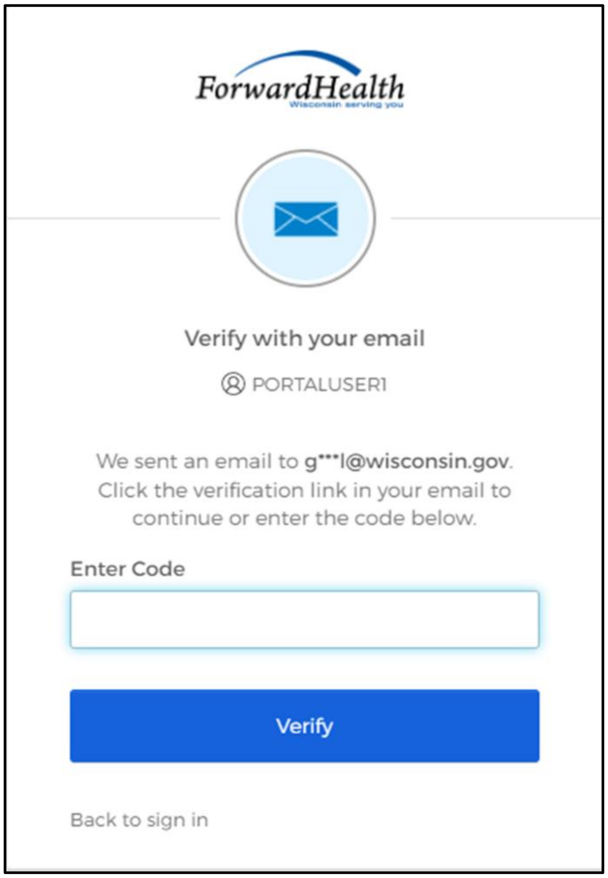


Figure 27 Verify With Your Email Box

The Reset your Okta password box will be displayed.

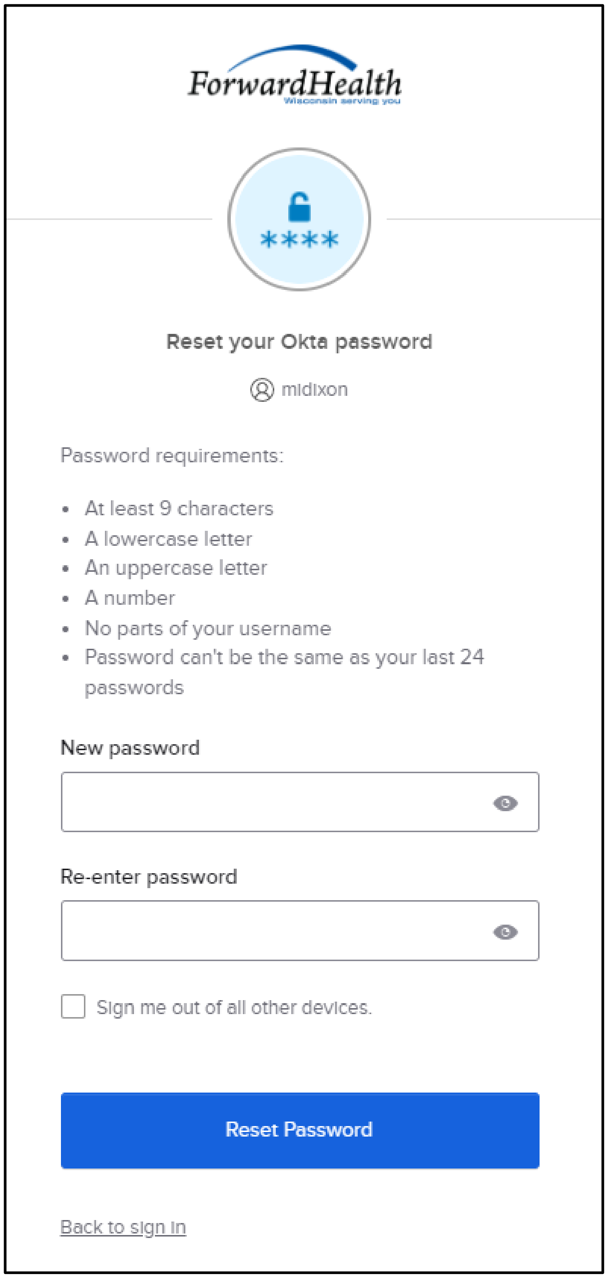


Figure 28 Reset Your Okta Password Box

11. Enter a new password (twice for confirmation).
12. Click **Reset Password**. The password will be changed and the user will be logged in to the secure Portal.

3.4 Unlocking An Account

1. Access the Portal at https://www.forwardhealth.wi.gov/.
2. Click **Login**. A sign In box will be displayed.

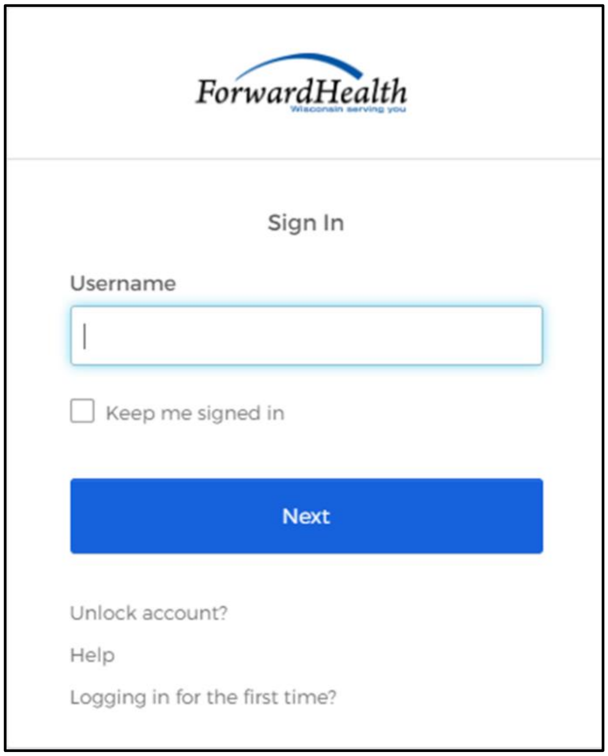


Figure 29 Sign In Box

3. Click **Unlock account?**

An Unlock account box will be displayed.

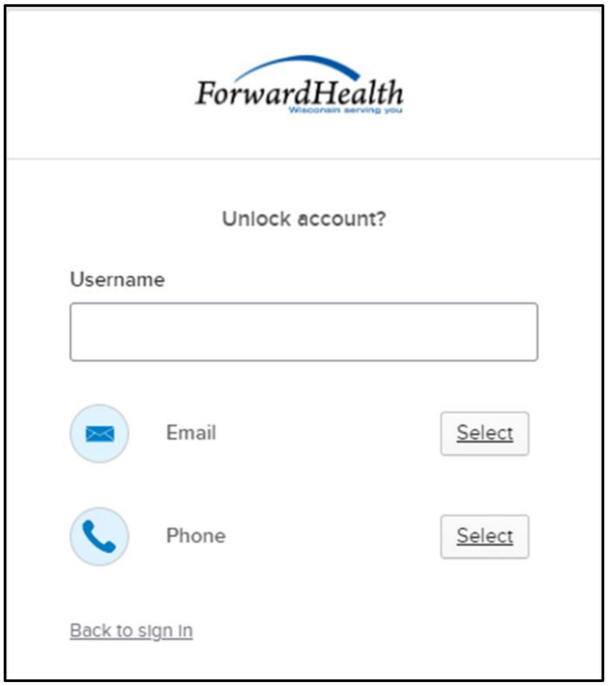


Figure 30 Unlock Account Box

4. Enter the user's username.
5. Click **Select** to receive a verification via email or phone.

- If the user clicks **Select** for email:

   a. A Get a verification email box will be displayed.

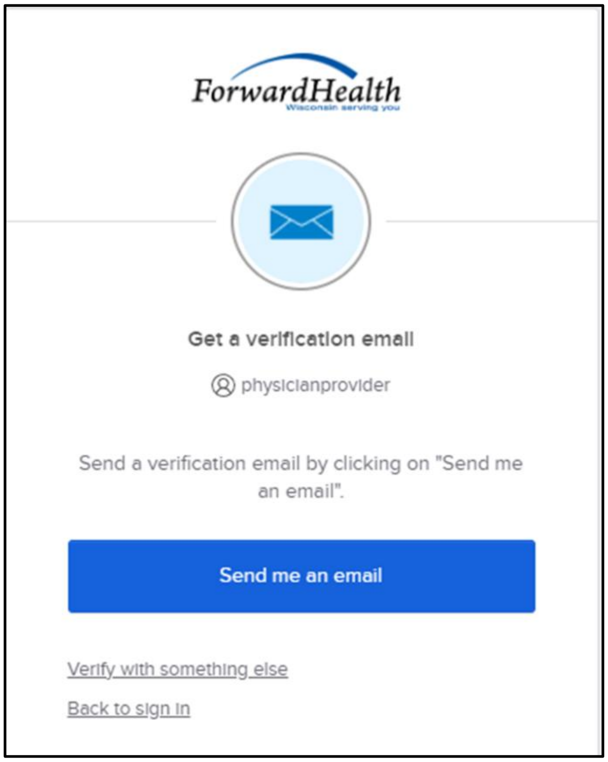


Figure 31 Get A Verification Email

   b. Click **Send me an email**. Note: The user also has the option to select **Verify with something else** which will take them back to the Unlock account box or **Back to sign in** which will take them back to the sign in page.

A verify with your email box will be displayed and an email will be sent.

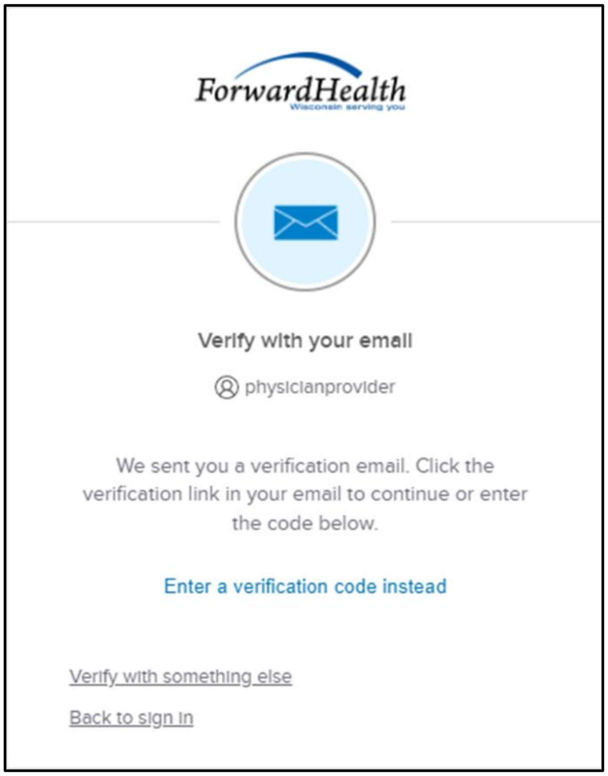


Figure 32 Verify With Your Email Box

c. Proceed to Step 6.

- If the user clicks **Select** for phone:

  a. A verify with your phone box will be displayed.

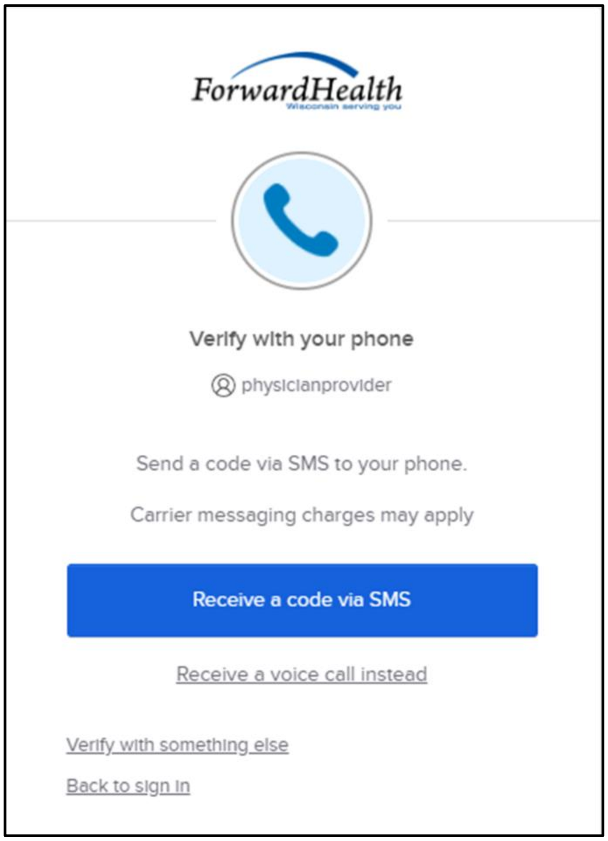


Figure 33 Verify With Your Phone Box

  b. Click **Receive a code via SMS** (text) or **Receive a voice call instead**. Note: The user also has the option to select **Verify with something else**, which will take them back to the Unlock account box, or **Back to sign in**, which will take them back to the sign in page.

A Verify with your phone box will be displayed.

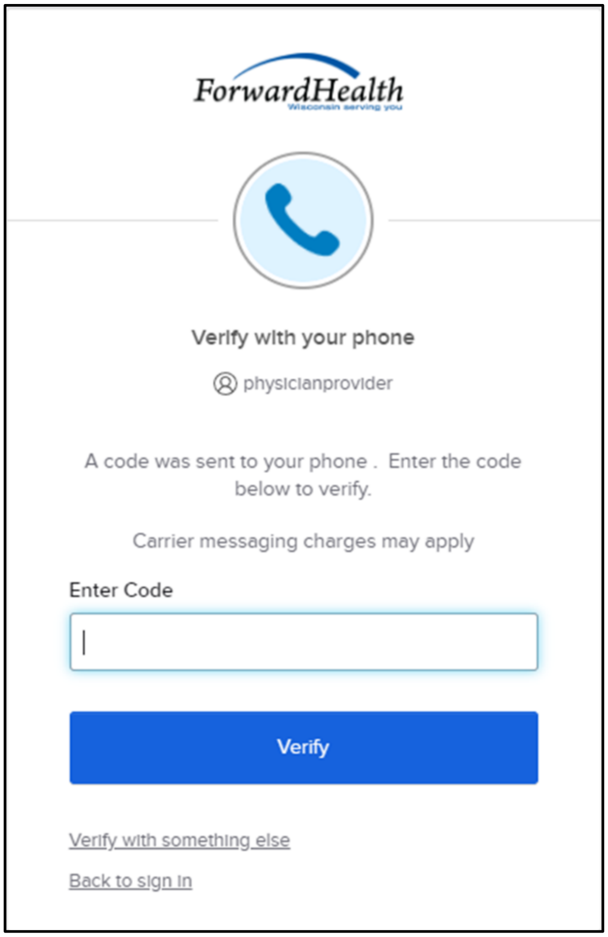


Figure 34 Verify With Your Phone Box

c. Enter the code that was sent.

d. Click **Verify**.

A Get a verification email box will be displayed.

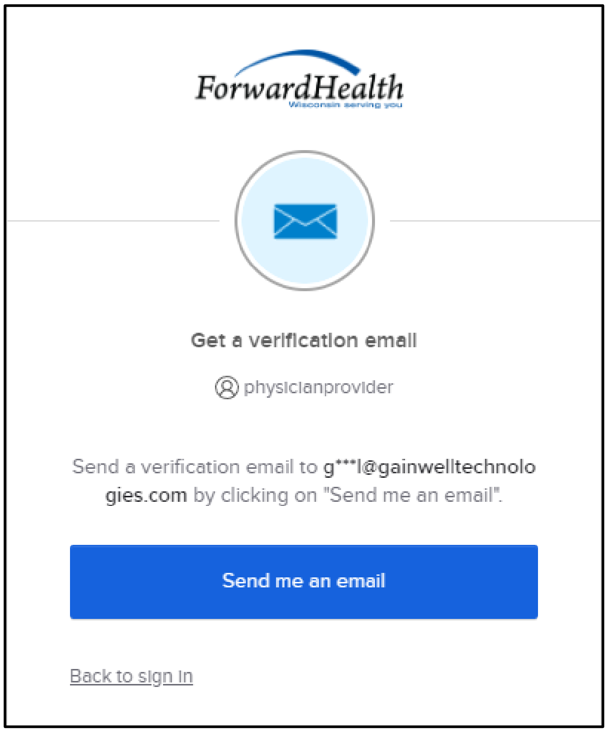


Figure 35 Get a Verification Email Box

e. Click **Send me an email**.

A Verify with your email box will be displayed and an email will be sent.

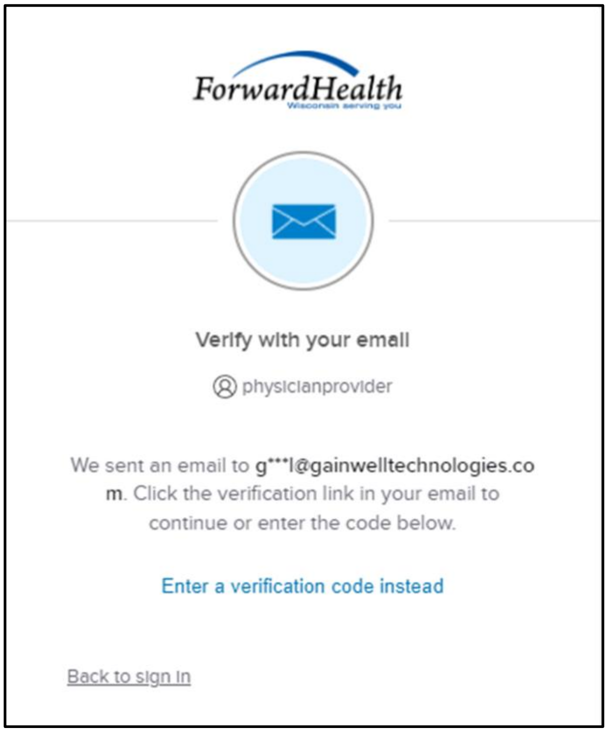


Figure 36 Verify With Your Email Box

6. The email sent to the user's email address includes an **Unlock Account** link (Option 1) and a verification code (Option 2).

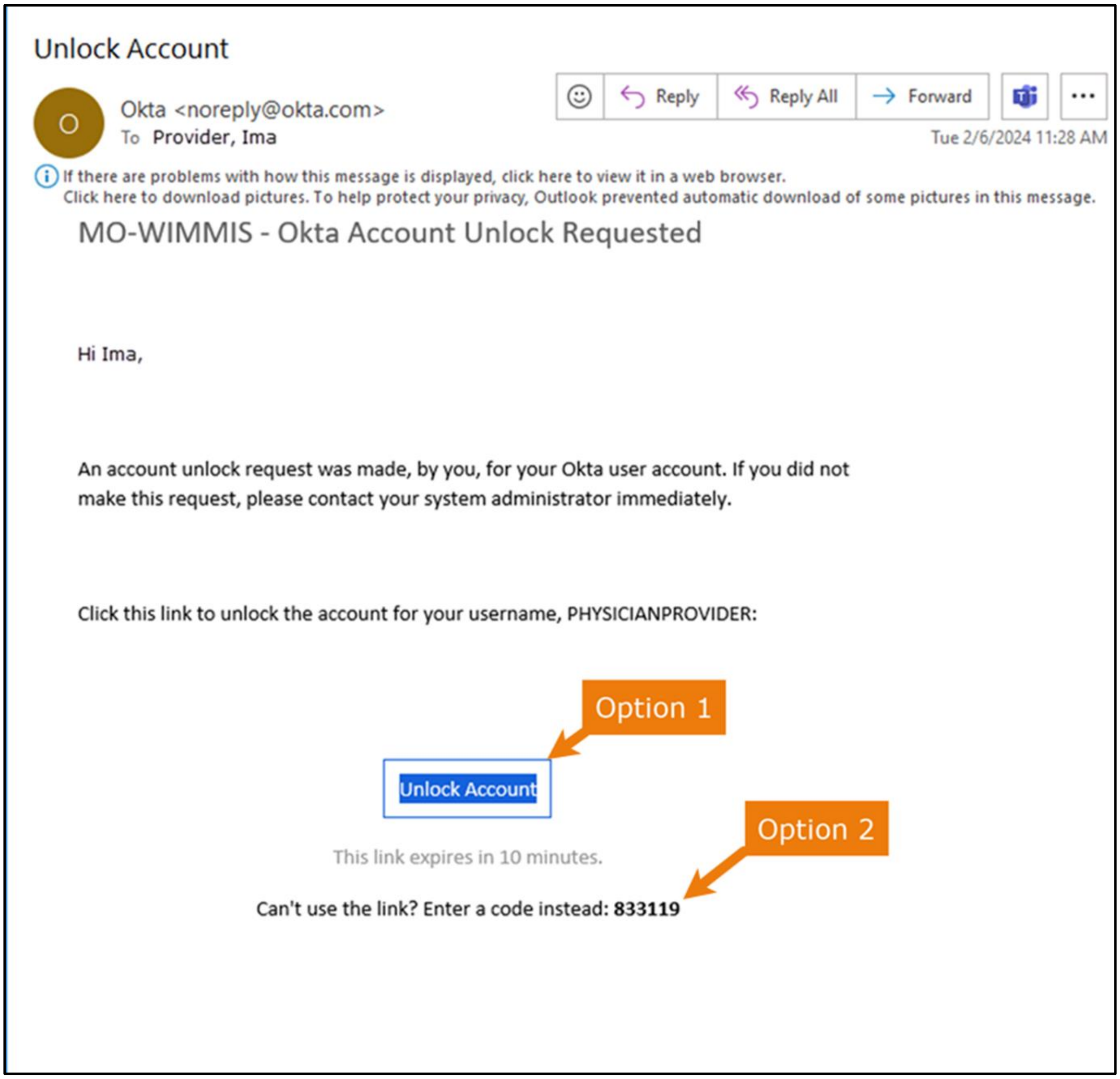


Figure 37 One-Time Verification Code Email

7. The user can choose to either click the **Unlock Account** link (Option 1) or enter the verification code from the email (Option 2) instead.

- Clicking the **Unlock Account** link from the email will display a verification code box.

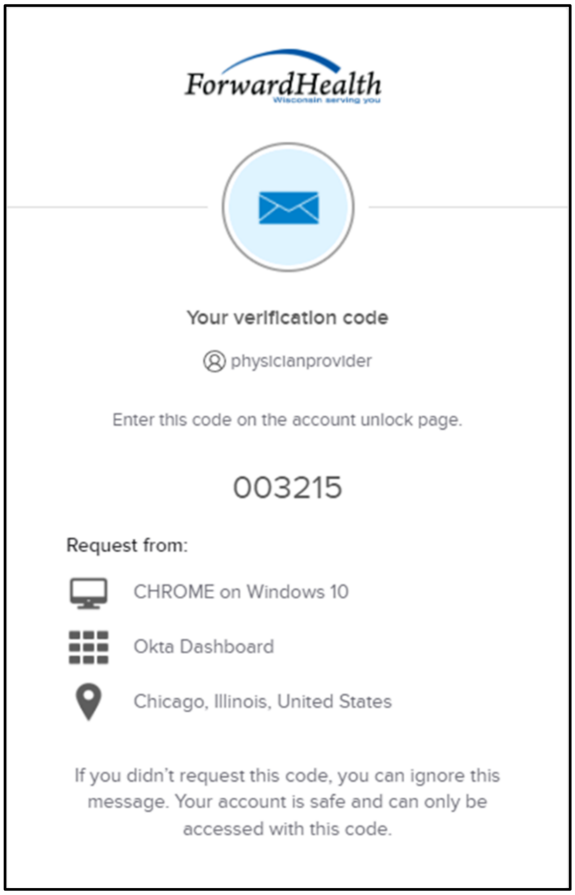


Figure 38 Verification Code Box

8. Copy the verification code from the verification code box or from the unlock account email, return to the verify with your email box, and click **Enter a verification code instead**.
9. Enter the code from the verification code box or from the unlock account email and click **Verify**.

A Verify with your password box will be displayed with a message stating the account has been successfully unlocked.

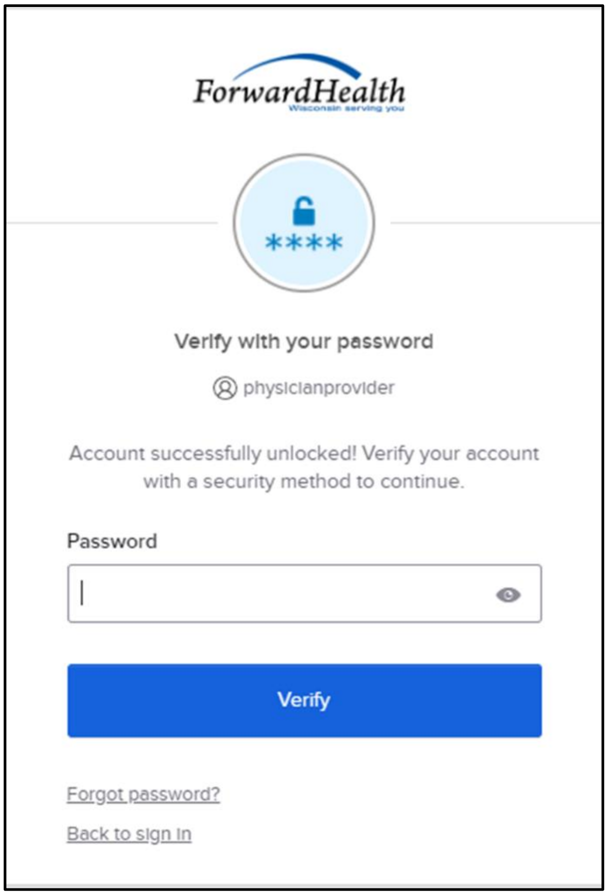


Figure 39 Verification Code Box

10. Click **Back to sign in** to log in.

4 Maintenance

Users may change account information such as contact name, phone number, or email address through the Maintenance link on the Account homepage.

4.1 Change Account Information

1. Access the Portal at https://www.forwardhealth.wi.gov/.
2. Click **Login**. A Sign In box will be displayed.

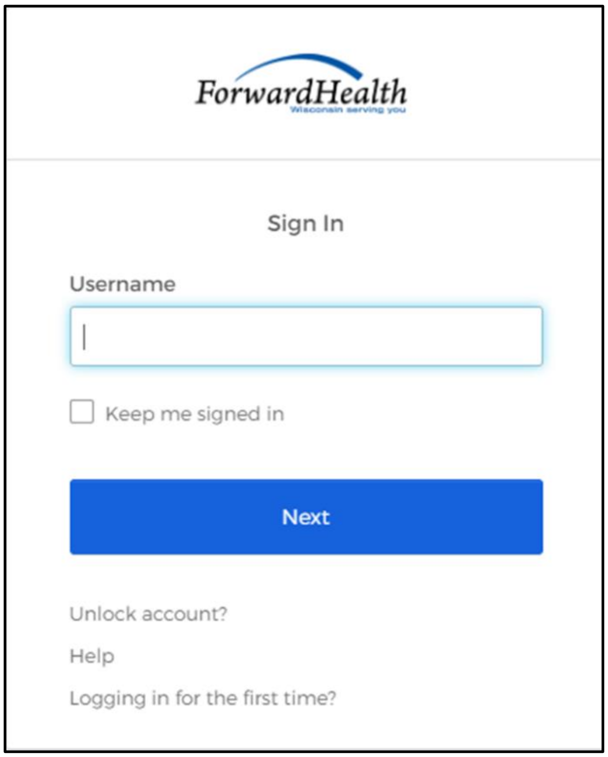


Figure 40 Sign In Box

3. Enter the user's username.
4. Click **Next**.

A Verify with your password box will be displayed.

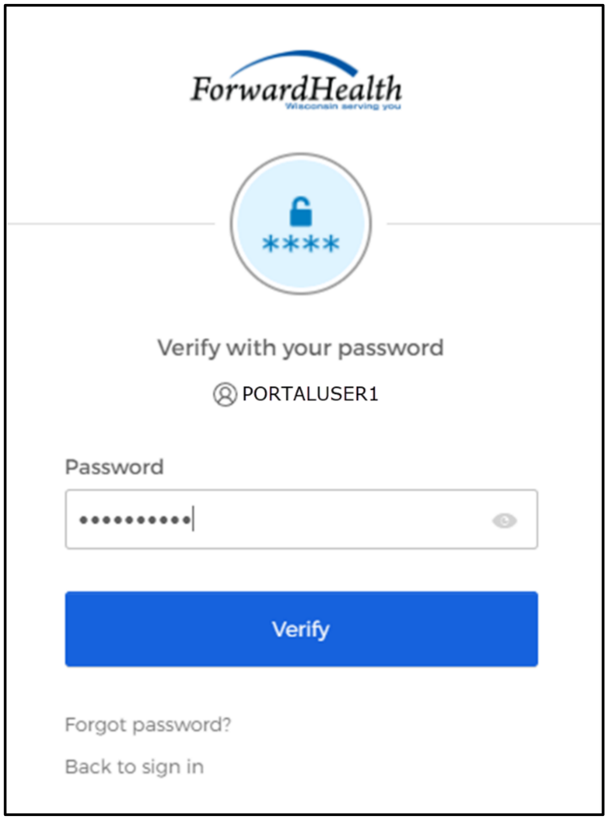


Figure 41 Verify With Your Password Box

5. Enter the user's password. The user's password is case sensitive. Make certain to enter it exactly.
6. Click **Verify**.

The secure Provider page will be displayed.

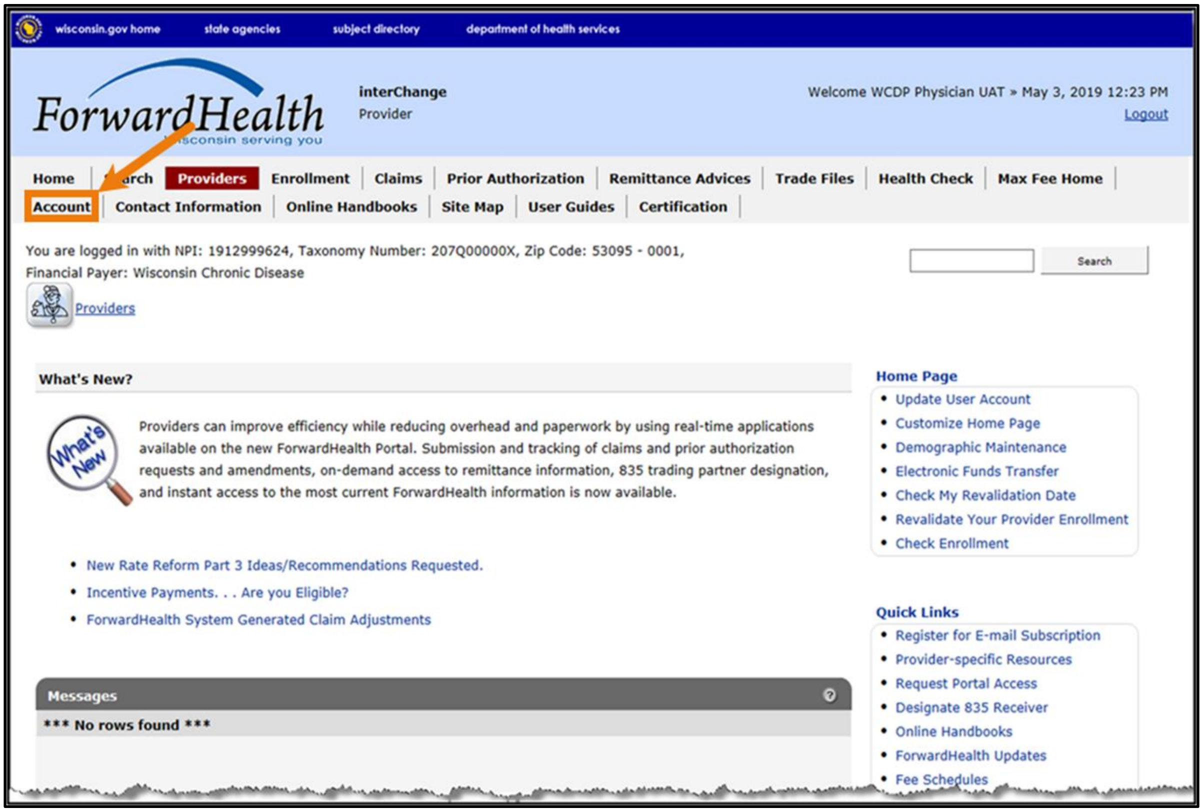
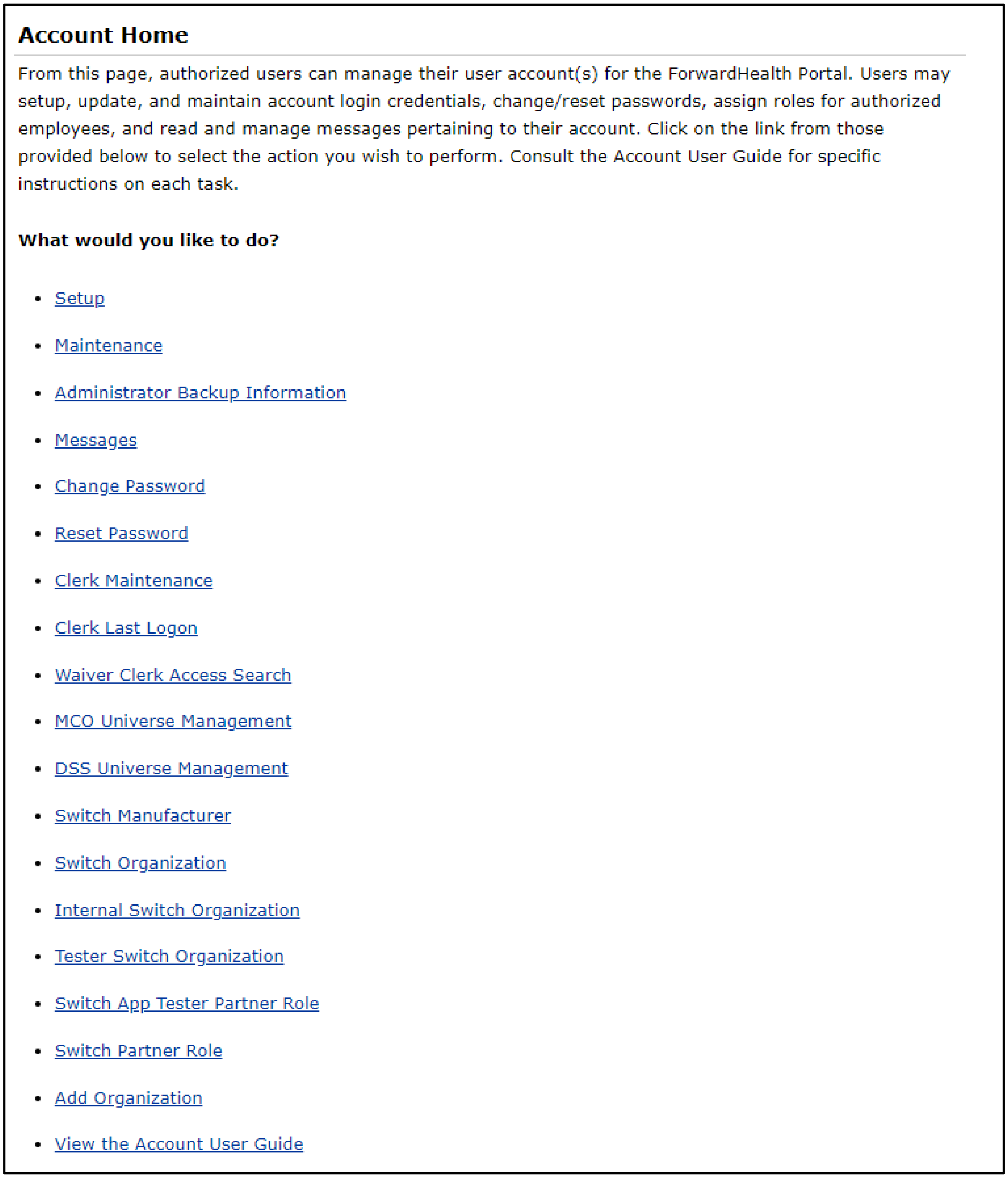


Figure 42 Secure Provider Homepage

7. Click **Account** on the main menu at the top of the page. The Account Home page will be displayed.



Account Home

From this page, authorized users can manage their user account(s) for the ForwardHealth Portal. Users may setup, update, and maintain account login credentials, change/reset passwords, assign roles for authorized employees, and read and manage messages pertaining to their account. Click on the link from those provided below to select the action you wish to perform. Consult the Account User Guide for specific instructions on each task.

What would you like to do?

- Setup
- Maintenance
- Administrator Backup Information
- Messages
- Change Password
- Reset Password
- Clerk Maintenance
- Clerk Last Logon
- Waiver Clerk Access Search
- MCO Universe Management
- DSS Universe Management
- Switch Manufacturer
- Switch Organization
- Internal Switch Organization
- Tester Switch Organization
- Switch App Tester Partner Role
- Switch Partner Role
- Add Organization
- View the Account User Guide

Figure 43 Account Home Page

Various account management functions can be performed using the links on the Account Home page.

8. Click **Maintenance**. The Account Maintenance panel will be displayed.

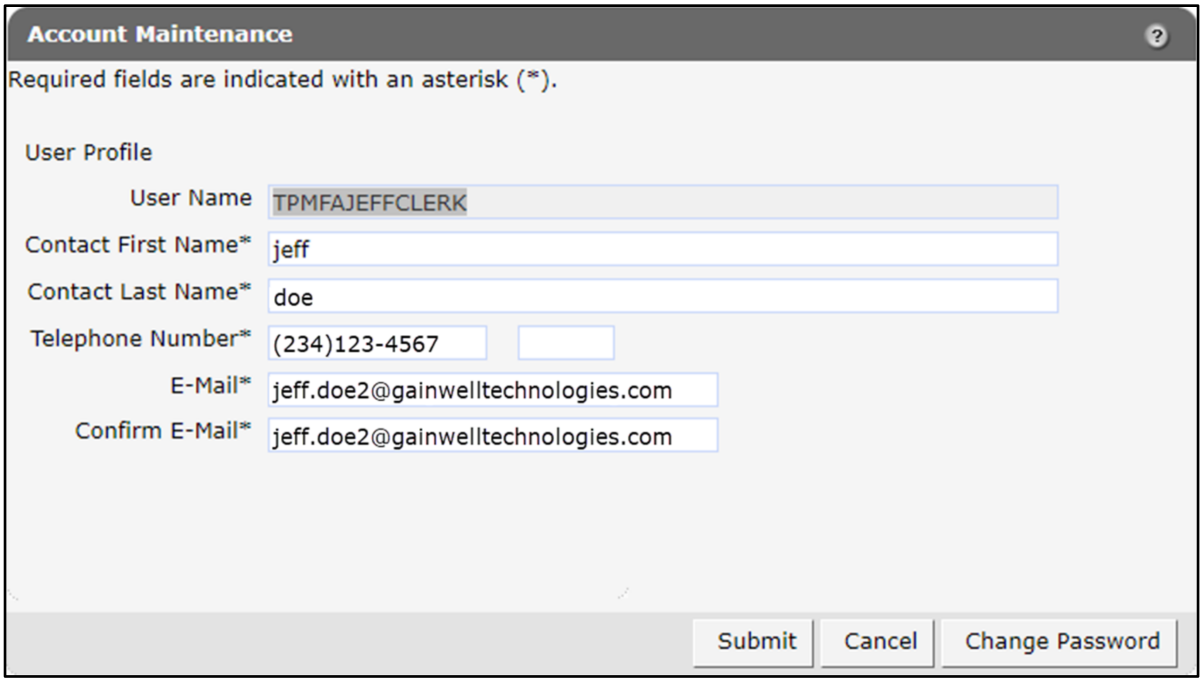


Figure 44 Account Maintenance Panel

9. Make applicable changes.

10. Click **Submit**. An Account Maintenance verification panel will be displayed if the phone number or email address were changed.

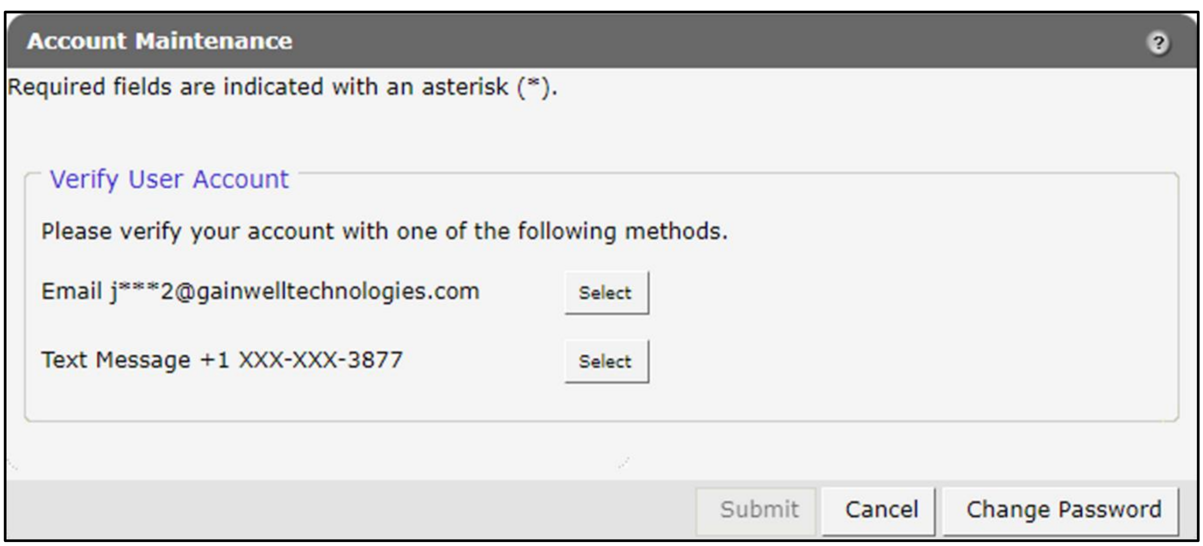


Figure 45 Account Maintenance Panel – Verify User Account

11. Select the email or text message to verify the account by clicking **Select** after the appropriate method. An Account Maintenance verification panel will be displayed.

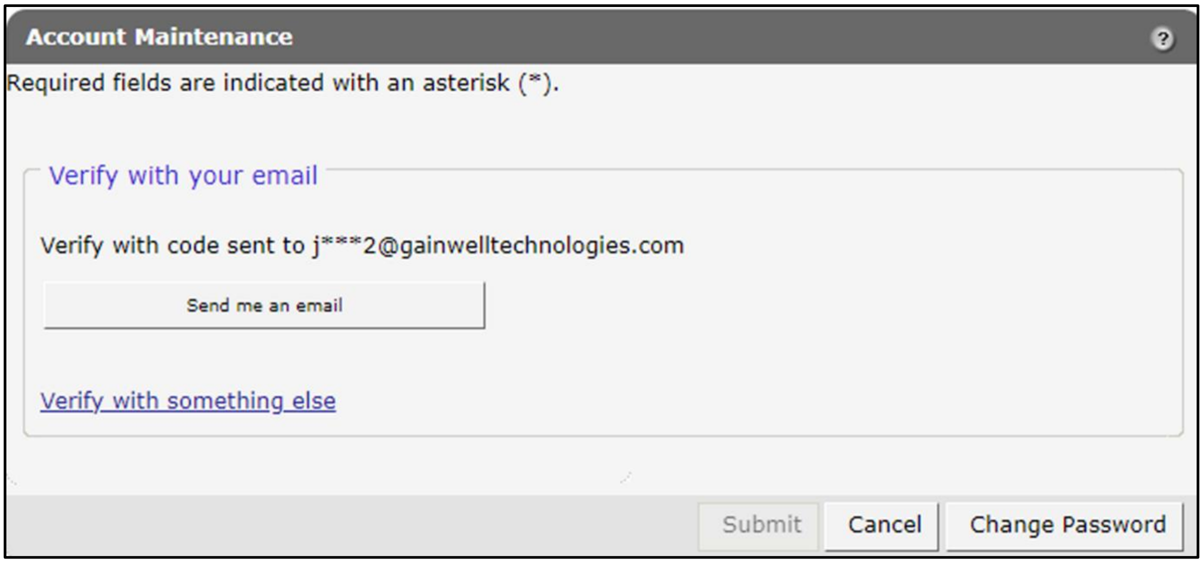


Figure 46 Account Maintenance Panel – Email or Text Message Verification

12. Click **Send me an email** for an email or **Receive a code via SMS** for a text. Note: Clicking **Verify with something else** will direct the user back to the verify user account screen allowing verification by either email or text message.

13. Enter the code in the Account Maintenance verification panel.

Figure 47 Account Maintenance Panel – Enter Code

14. Click **Verify**. A confirmation message will be displayed.

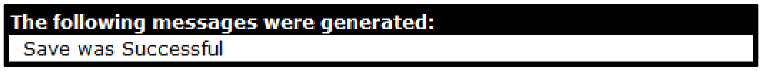


Figure 48 Confirmation Message

5 Change Password

Users will be prompted to change their Portal account passwords every 60 days; however, through the Change Password function, users can change their password at any time.

Note: The Change Password link on the Account Home page serves the same purpose as the Change Password button on the Account Maintenance page.

1. On the Account Home page, click **Change Password**. The Change Password page will be displayed.

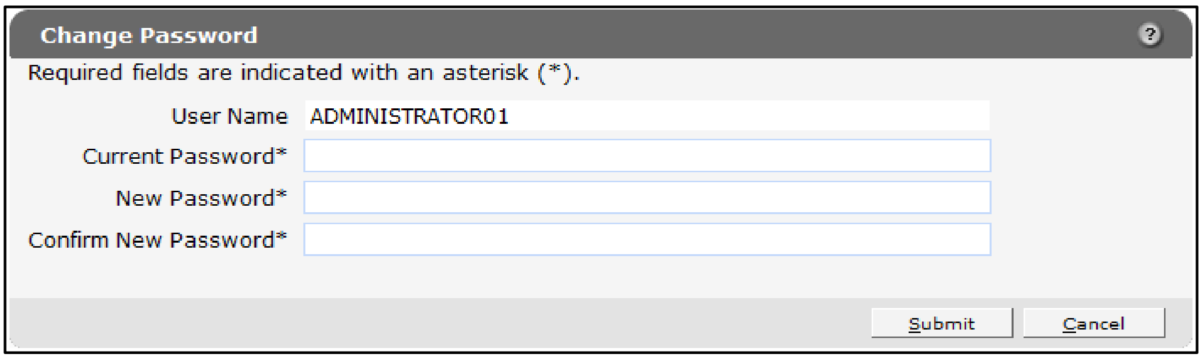


Figure 49 Change Password Page

2. Enter the user's current password.
3. Enter the user's new password (twice for confirmation). The password must be between nine–15 characters and must contain three different types of characters such as uppercase letters, lowercase letters, special characters, or numbers. The password must be unique and cannot contain information from the user name, contact first name, or contact last name.

   Note: The new password cannot match any of the last 24 passwords.
4. Click **Submit**. A Change Password verification panel will be displayed.

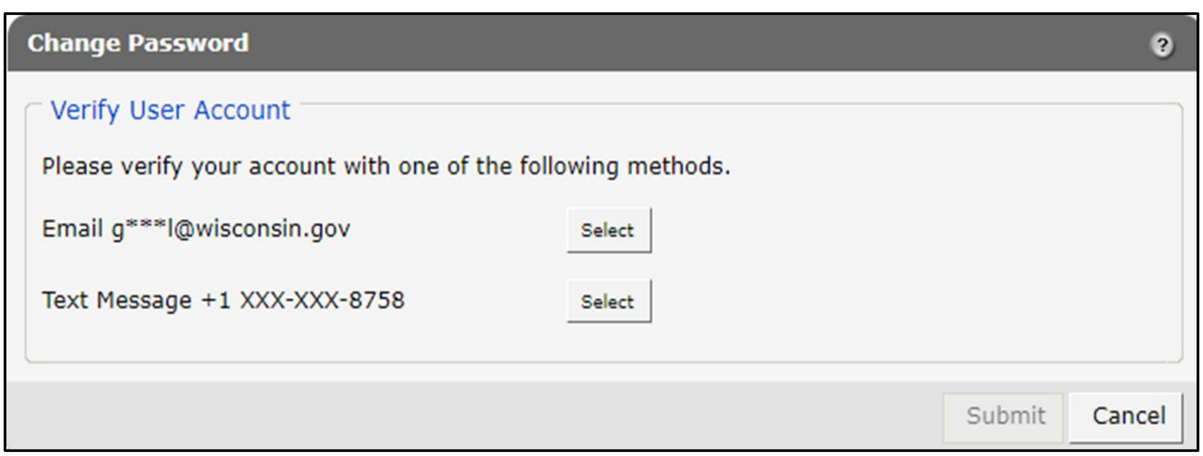


Figure 50 Change Password Panel – Verify User Account

5. Select the email or text message to verify the account by clicking **Select** after the appropriate method. A Change Password verification panel will be displayed.

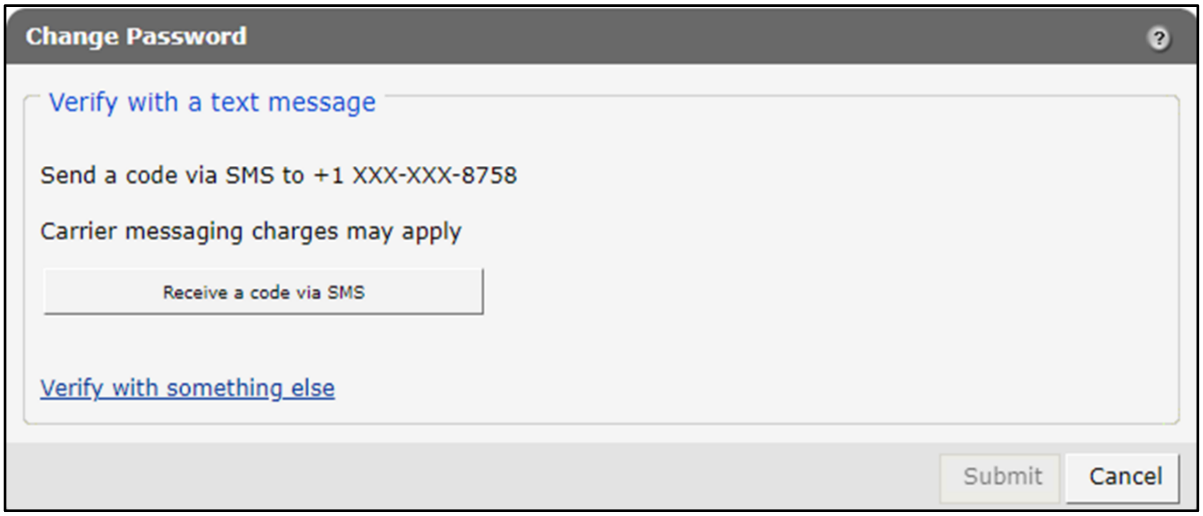


Figure 51 Change Password Panel – Email or Text Message Verification

6. Click **Receive a code via SMS** for a text or **Send me an email** for an email. Note: Clicking **Verify with something else** will direct the user back to the verify user account screen allowing verification by either email or text message**.**

7. Enter the code in the Change Password verification panel.

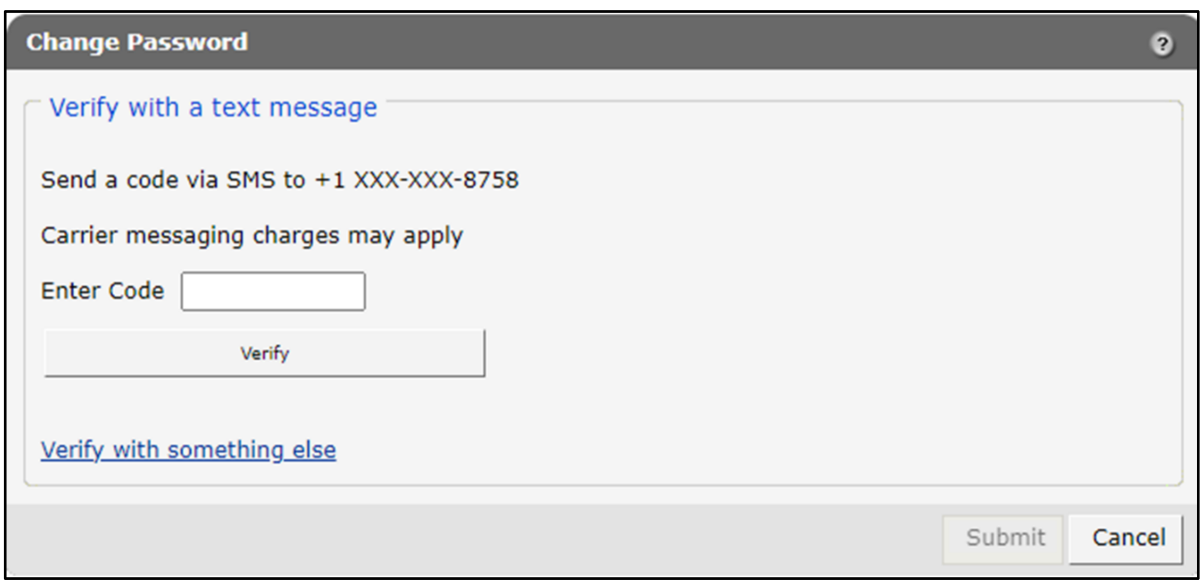


Figure 52 Change Password Panel – Enter Code

8. Click **Verify**. A confirmation message will be displayed.

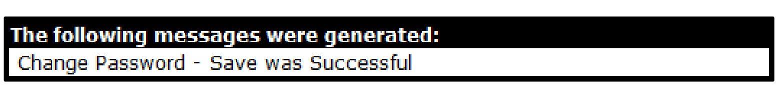


Figure 53 Confirmation Message

6 Clerk Maintenance

If more than one person will be working on the account, clerk accounts must be established and roles assigned for the various functions the clerks will be performing.

Note: Clerk users with established accounts that have been inactive for at least 60 days will be notified as follows:

- Inactive for 60 days—Notification will be sent indicating clerk inactivity.
- Inactive for 80 days—Notification will be sent pending automatic removal.

Accounts will automatically be removed after 90 days of inactivity.

On the Account page, click **Clerk Maintenance**. The Clerk Maintenance Search panel will be displayed.

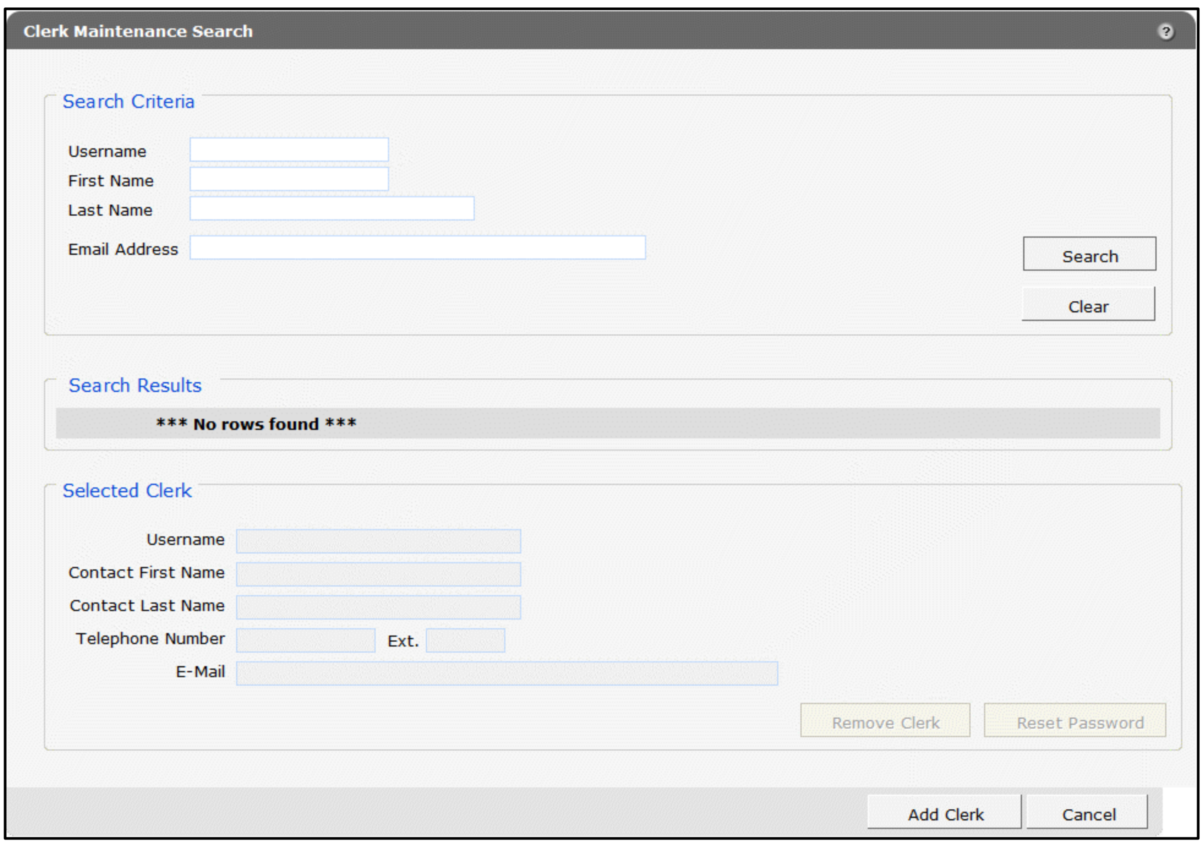


Figure 54 Clerk Maintenance Search Panel

Through the Clerk Maintenance panels, users with administrative and clerk administrative accounts can search for, add, or remove clerks; assign clerk roles; and reset a clerk's password.

Note: Users with clerk administrative accounts may not administer their own accounts or other administrative or clerk administrative accounts.

6.1 Add a Clerk

The Add Clerk function allows the user to add new clerks to a provider organization and to assign specific roles.

1. Click **Add Clerk** located at the bottom of the Clerk Maintenance Search panel. The Clerk Account panel will be displayed.

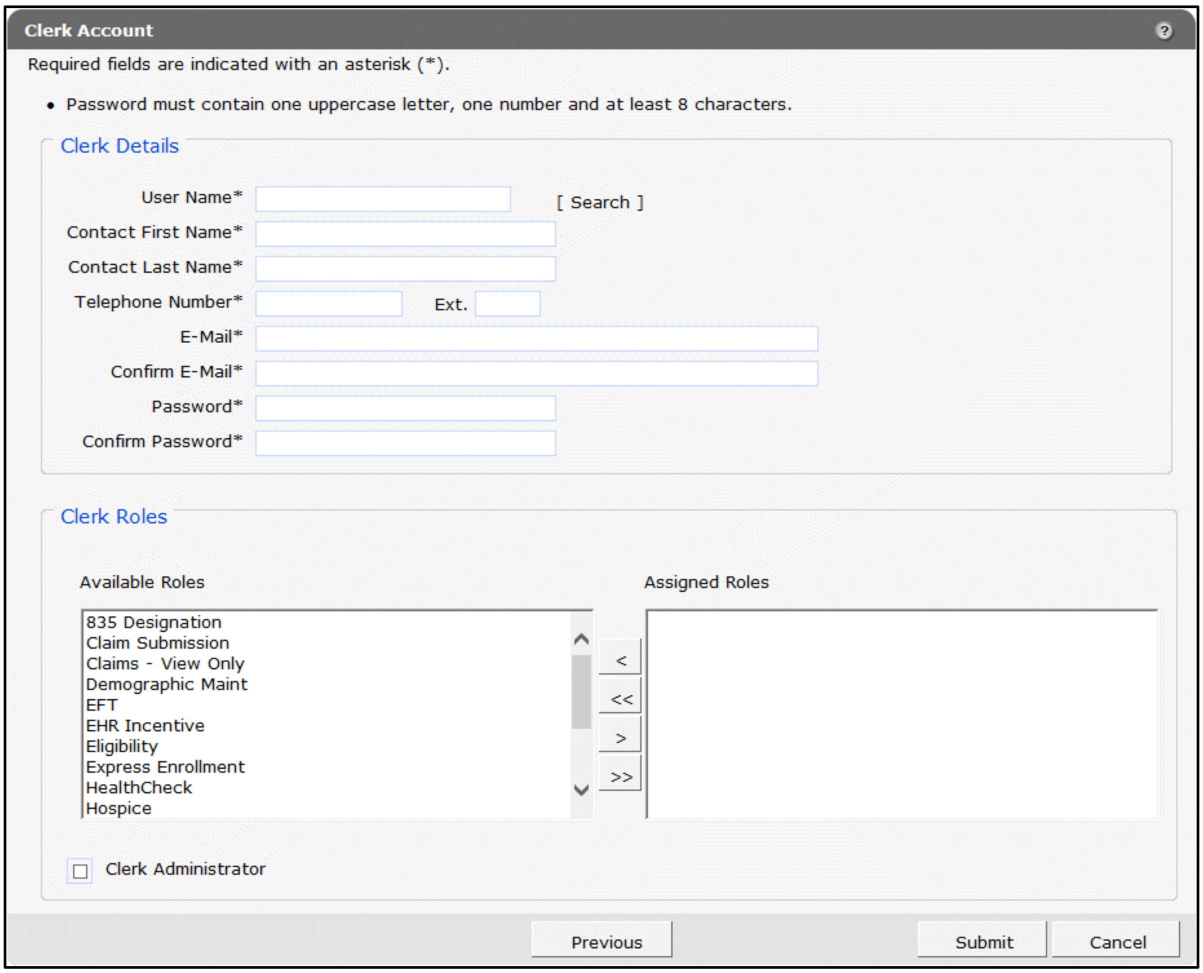


Figure 55 Clerk Account Panel

Complete the following steps to add a new clerk account:

- Enter a user name. The user name must be between six–20 characters and can only contain letters and numbers. The user name is not case-sensitive.
- Enter the new clerk’s contact first name and contact last name.
- Enter the new clerk’s phone number (and extension, if applicable).

- Enter the new clerk's email (twice for confirmation).
- Enter an initial password for the new clerk (twice for confirmation).

  The password must be between nine–15 characters and must contain three different types of characters such as uppercase letters, lowercase letters, special characters, or numbers. The password must be unique and cannot contain information from the user name, contact first name, or contact last name.

  Note: Clerks must change the password set up by the administrative account the first time they log in.

If adding a clerk account that has already been created but needs to be added to a new organization, complete the following steps:

- Click **Search** to the right of the User Name field. The User Name Search box will be displayed.

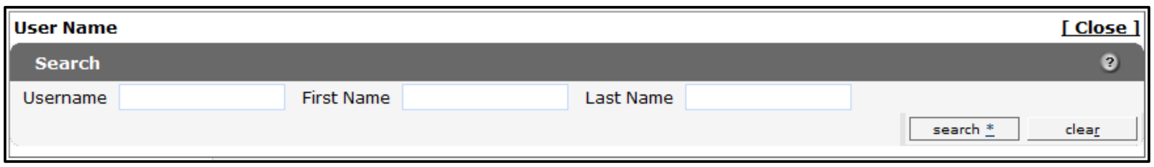


Figure 56 User Name Search Box

- Enter the clerk account's username, first name, or last name.
- Click **Search**. The clerk's information will be displayed in the "Clerk Details" section.

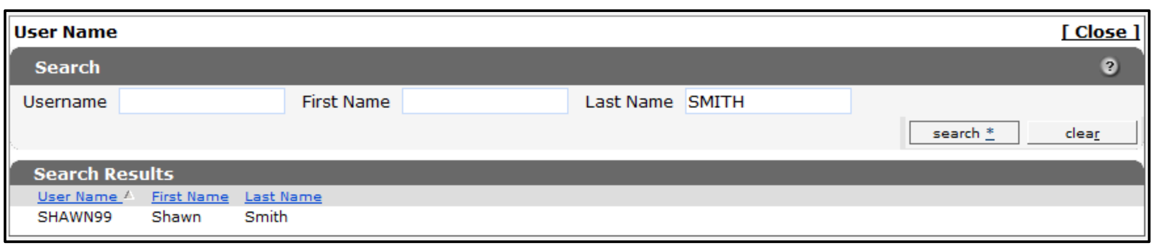


Figure 57 Search Results Section

- Click the row of the applicable clerk account. The User Name Search box will close and the clerk account information will be auto-populated in the “Clerk Details” section of the Clerk Account panel.

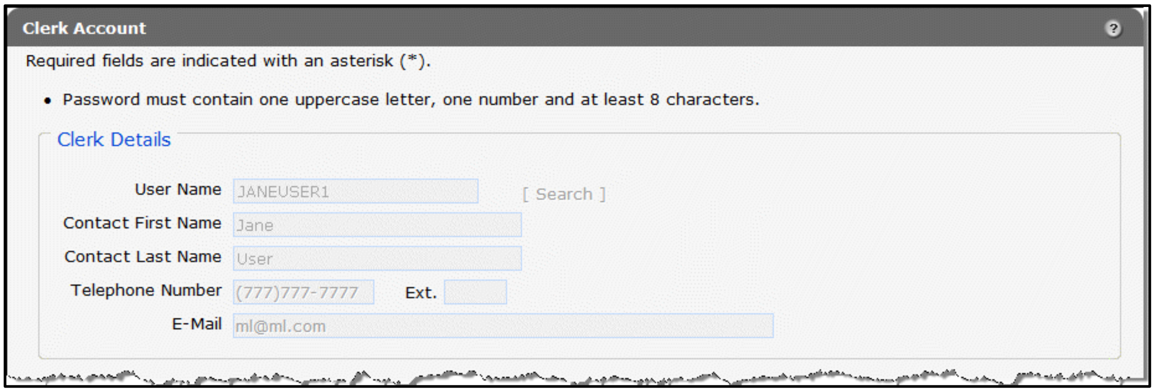


Figure 58 Clerk Account Information Auto-Populated on Clerk Account Panel

2. Proceed to the one of the following sections once clerk details have been entered or populated:

   - Step 2 of Section 6.3 Add a Role to a Clerk of this guide
   - Step 1 of Section 6.5 Assign a Clerk Administrator of this guide

6.2 Search for a Clerk

The Clerk Maintenance Search panel allows a user to select an existing clerk within the provider organization.

1. Enter information for the clerk in any combination in the Search Criteria section. Alternatively, leave the fields blank to bring up a list of all clerks associated with the provider organization.

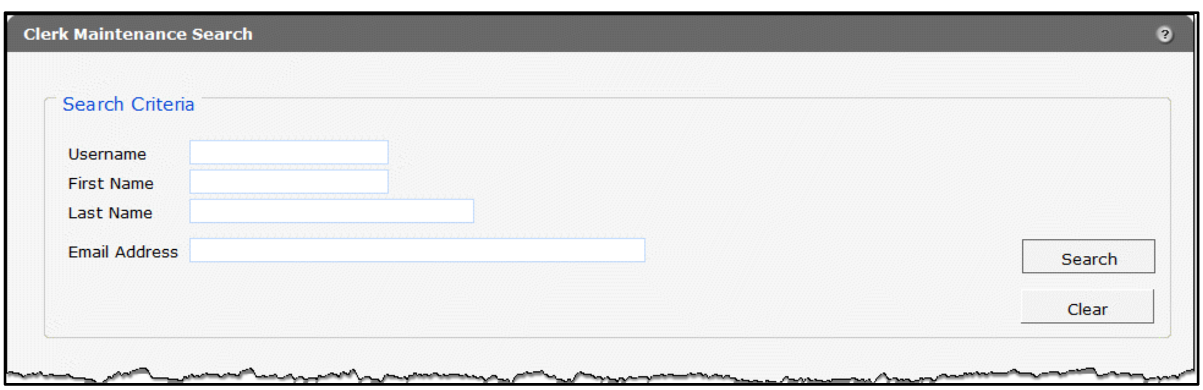


Figure 59 Search Criteria Section

2. Click **Search**.

3. Click the row containing the clerk's name in the "Search Results" section.

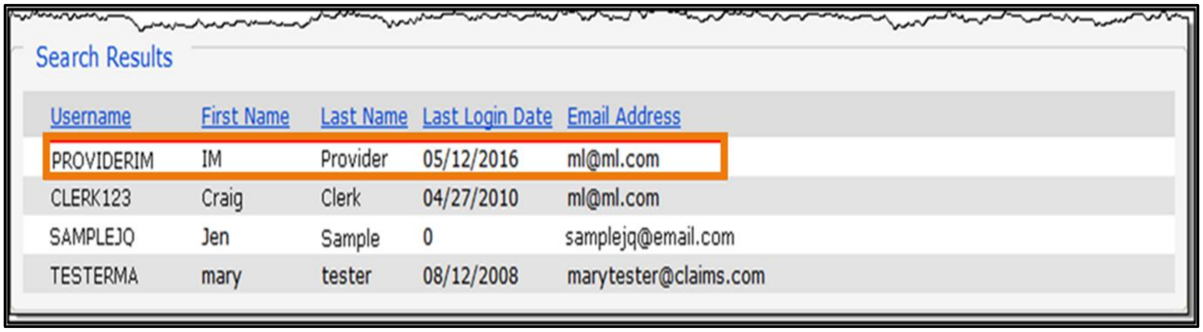


Figure 60 Search Results Section

The clerk's information will populate in the "Selected Clerk" section.

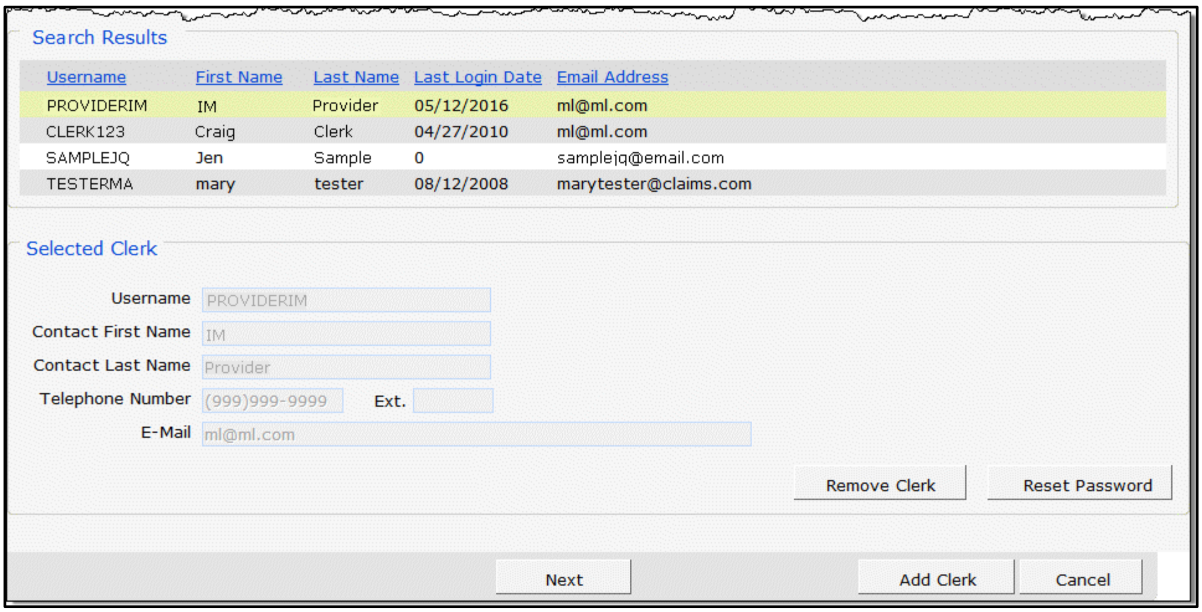


Figure 61 Search Results and Selected Clerk Sections

4. Proceed to one of the following sections of this guide once a clerk has been selected:

- Section 6.3 Add a Role to a Clerk
- Section 6.4 Remove a Role From a Clerk
- Section 6.5 Assign a Clerk Administrator
- Section 6.6 Reset a Clerk's Password
- Section 6.7 Delete a Clerk Account

6.3 Add a Role to a Clerk

The Clerk Roles function allows a user to add roles to new or existing clerks.

1. Click **Next**. The Clerk Account panel will be displayed.

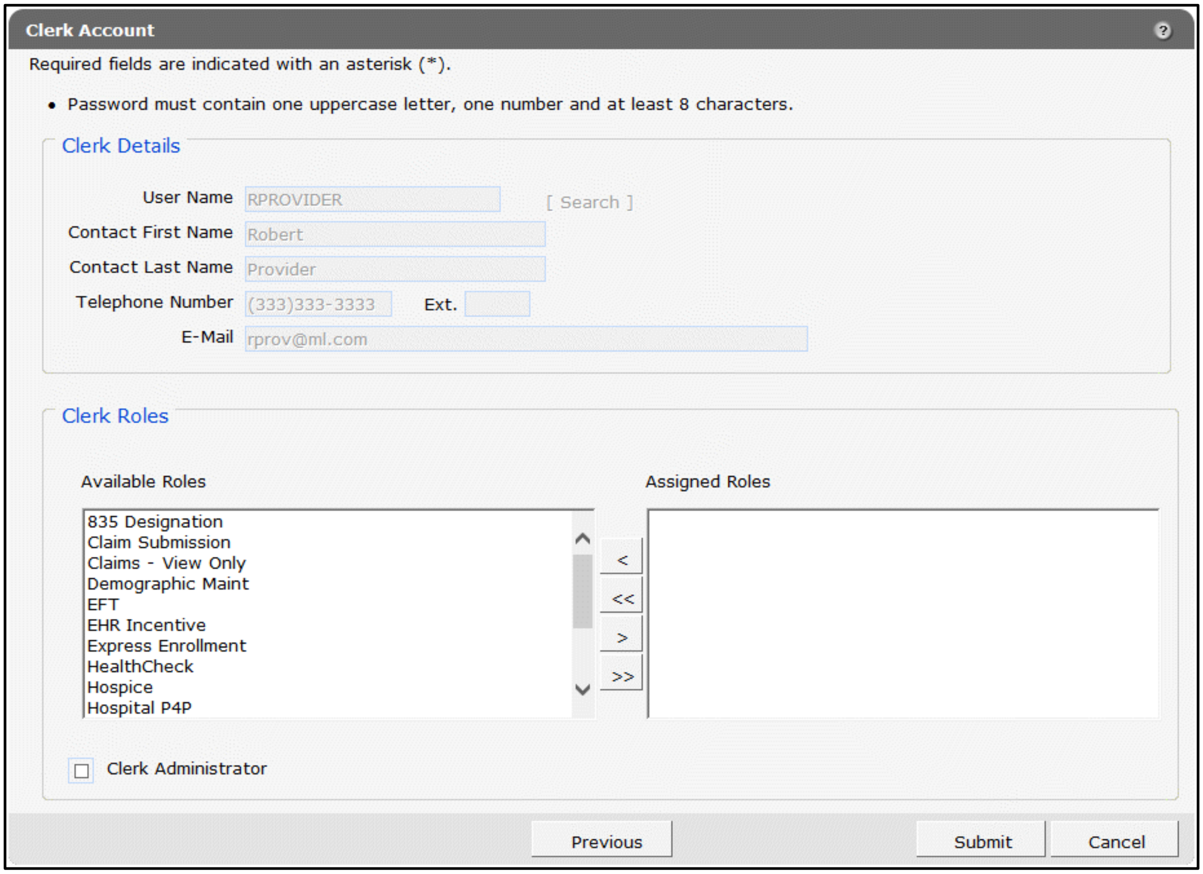


Figure 62 Clerk Account Panel

2. In the “Clerk Roles” section, select a role from the Available Roles box. To select more than one row, hold down the Ctrl key and click all applicable roles.

Figure 63 Clerk Roles Section With Available Roles

3. Click **>**. The selected role(s) will be added to the Assigned Roles box.

   Note: To add all available roles to the clerk, click **>>.**

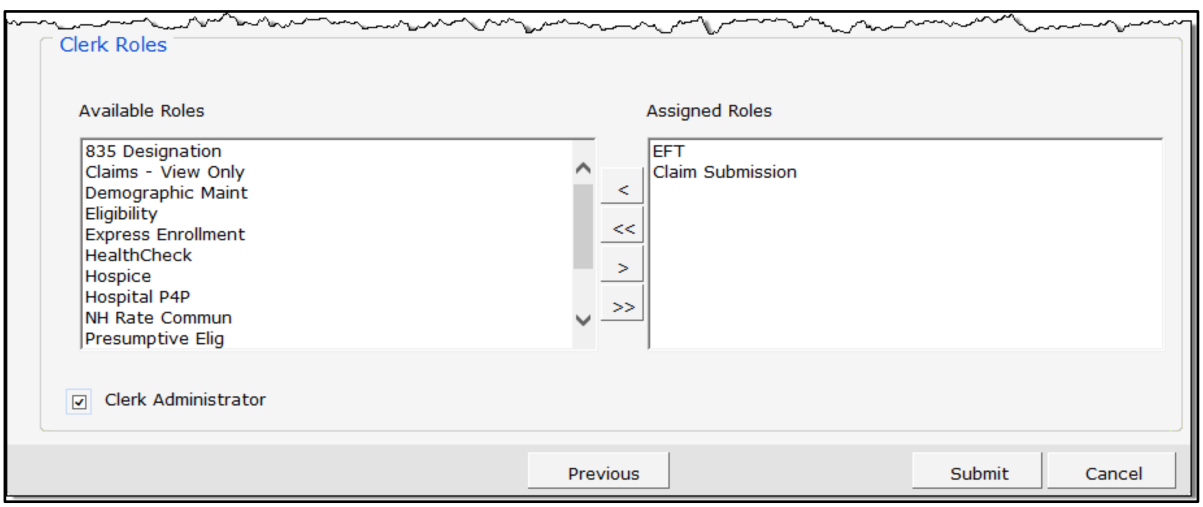


Figure 64 Clerk Roles Section With Assigned Roles

4. Click **Submit**. A confirmation message will be displayed at the top of the page.

Figure 65 User Successfully Updated Message

If an error message is received, correct the error(s) and click **Submit** again.

6.4 Remove a Role From a Clerk

1. Click **Next**. The Clerk Account panel will be displayed.

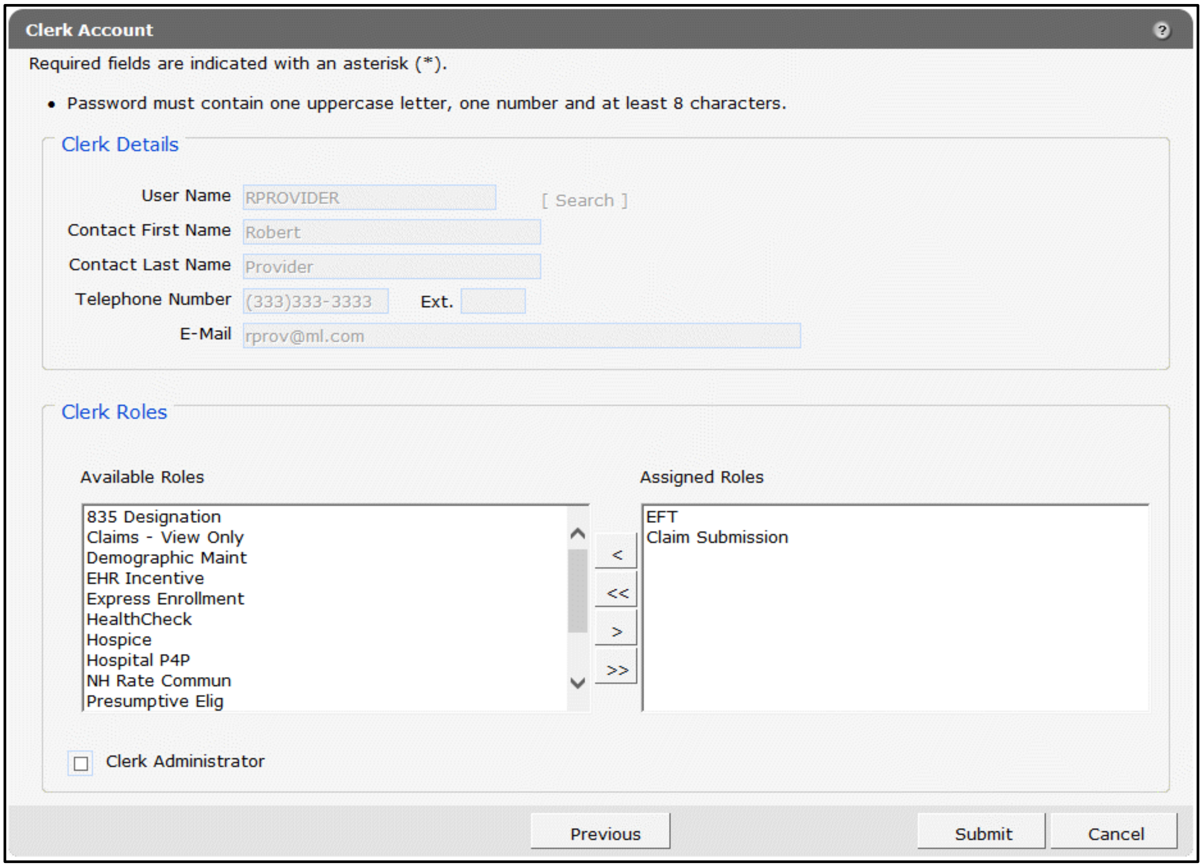


Figure 66 Clerk Account Panel

2. In the “Clerk Roles” section, select a role(s) from the Assigned Roles box. To select more than one row, hold down the Ctrl key and click all applicable roles.

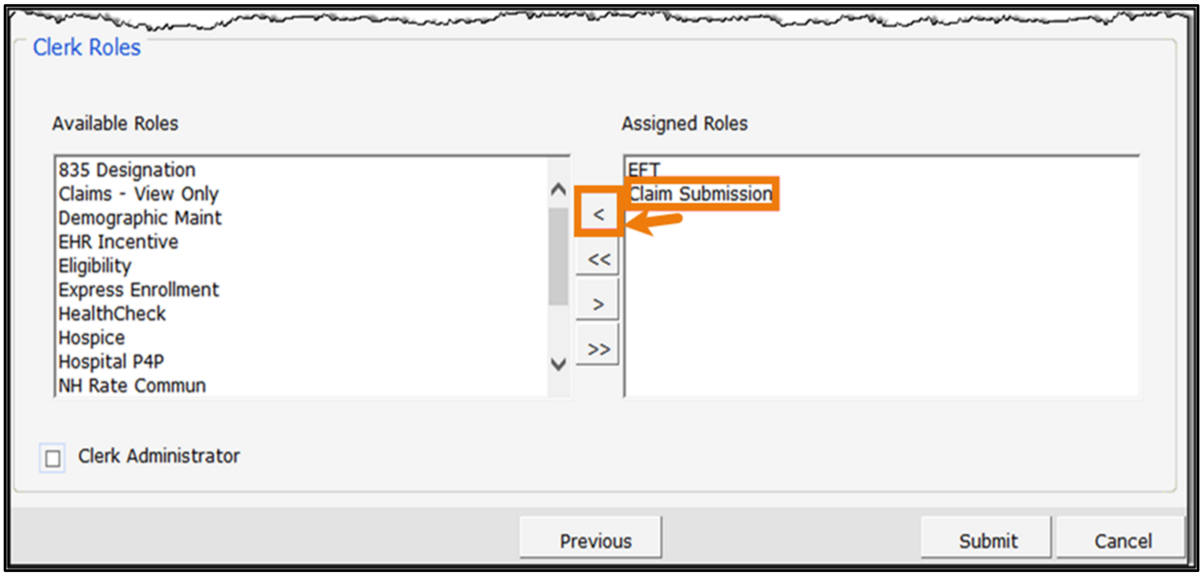


Figure 67 Clerk Roles Section With Assigned Roles

3. Click **<**. The selected role(s) will be transferred to the Available Roles box.

   Note: To remove all of a clerk’s assigned roles, click **<<.**

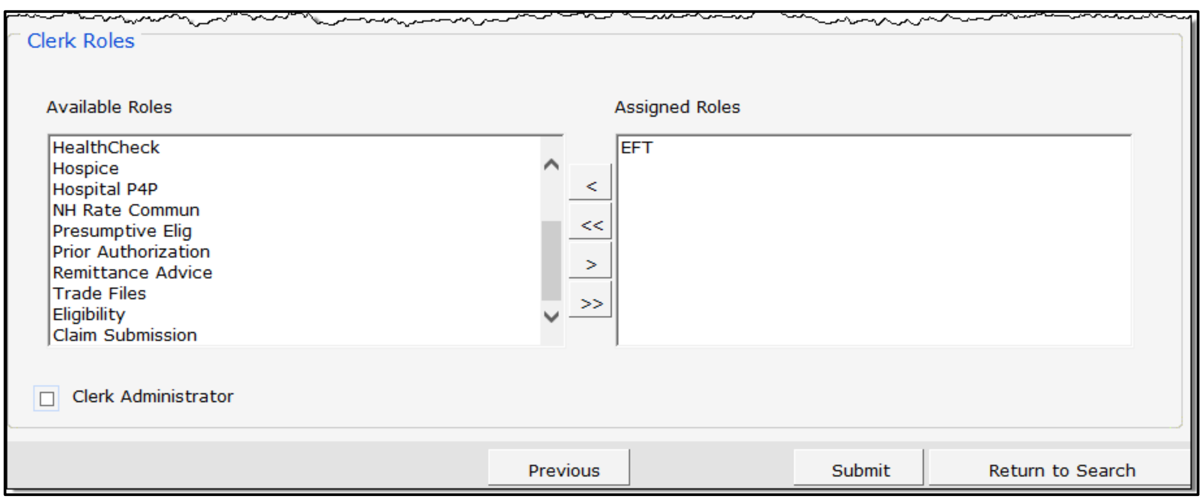


Figure 68 Clerk Roles Section With Role Removed

4. Click **Submit**. A confirmation message will be displayed at the top of the page.

Figure 69 Confirmation Message

   If an error message is received, correct the error(s) and click **Submit** again.

6.5 Assign a Clerk Administrator

The Clerk Administrator checkbox allows a user to assign a clerk administrative rights. A clerk with administrative rights can create accounts for clerks and manage the roles assigned to them.

1. Click **Next**. The Clerk Account panel will be displayed.

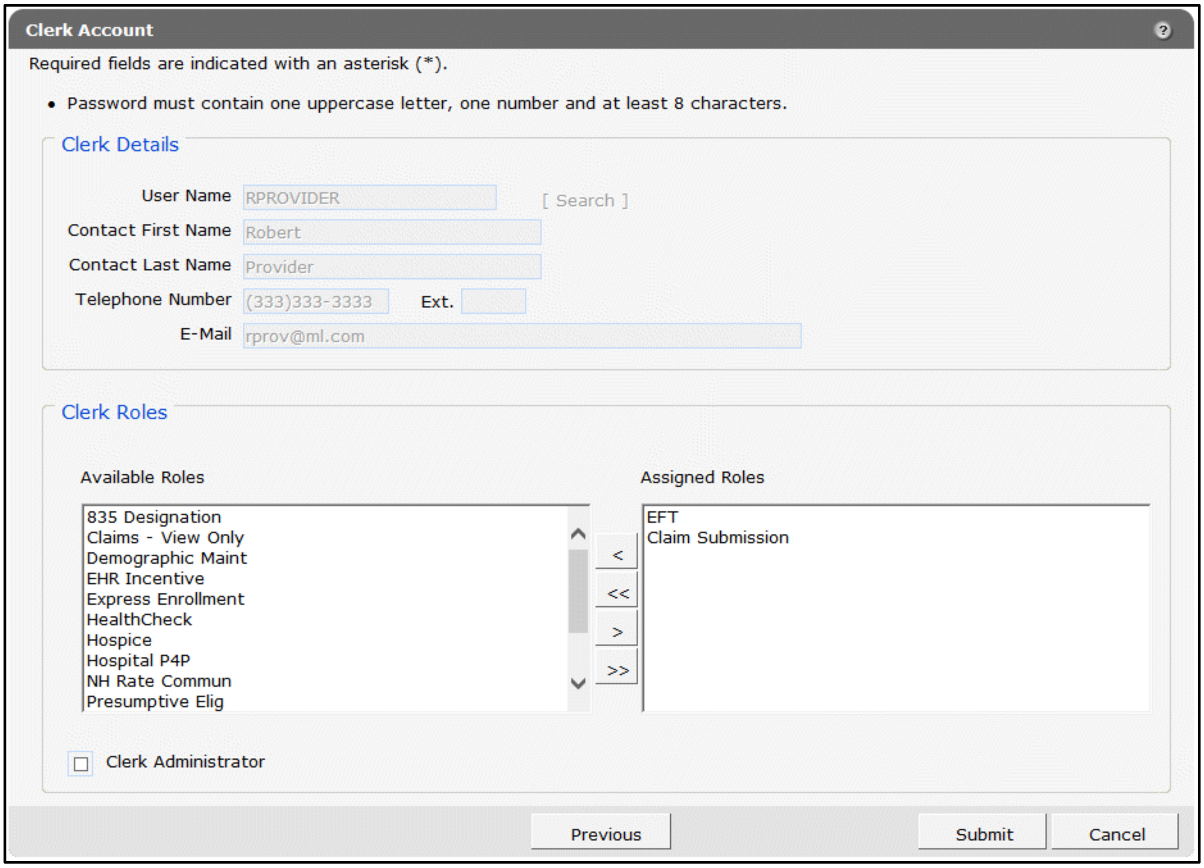


Figure 70 Clerk Account Panel

2. In the “Clerk Roles” section, check the Clerk Administrator box.

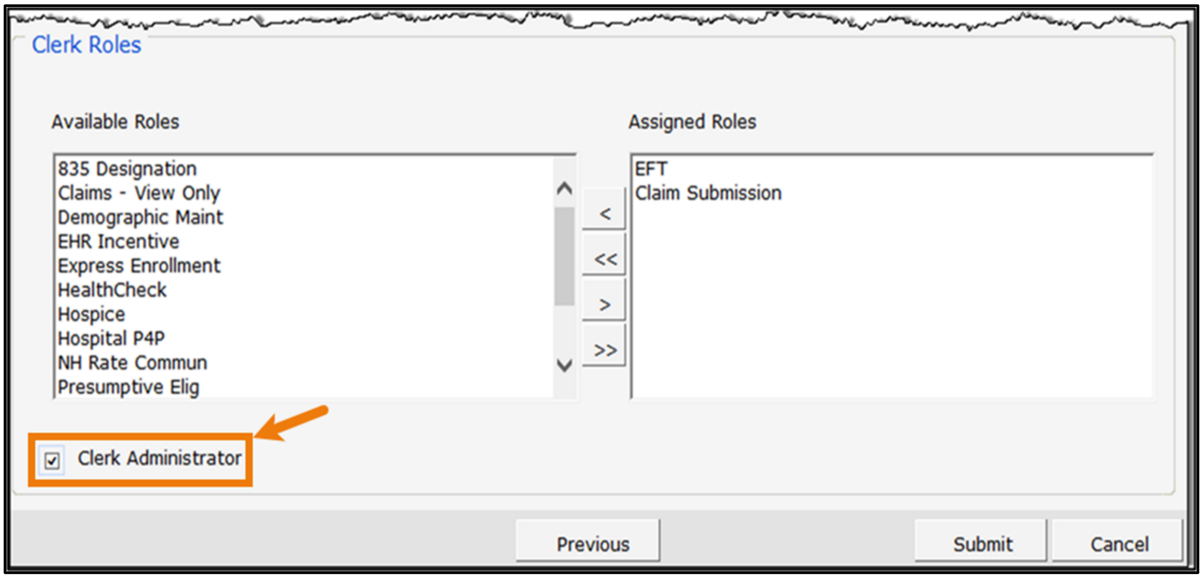


Figure 71 Clerk Roles Section With Clerk Administrator Checked

3. Click **Submit**. A confirmation message will be displayed at the top of the page.

Figure 72 Confirmation Message

6.6 Reset a Clerk’s Password

1. On the Clerk Maintenance Search panel, click **Reset Password**. The Reset Password page will be displayed.

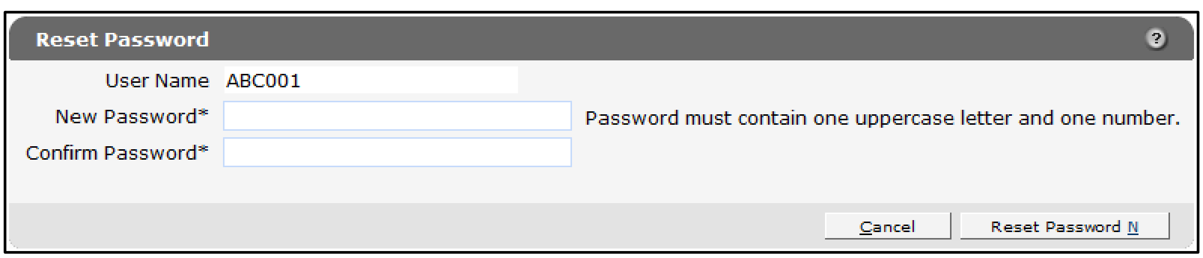


Figure 73 Reset Password Page

2. Enter the new password (twice for confirmation). The password must be between nine–15 characters and must contain three different types of characters such as uppercase letters, lowercase letters, special characters, or numbers. The password must be unique and cannot contain information from the user name, contact first name, or contact last name.

4. Click **Reset Password**. A confirmation message will be displayed at the top of the page.

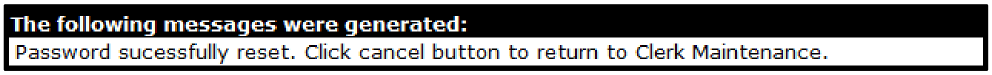


Figure 74 Confirmation Message

Note: Clerks must change the password set up by the administrative account the first time they log in.

If an error message is received, correct the error(s) and click **Reset Password** again.

6.7 Delete a Clerk Account

1. On the Clerk Maintenance Search panel, click **Remove Clerk** to initiate the record deletion. A dialog box confirming the deletion will be displayed.

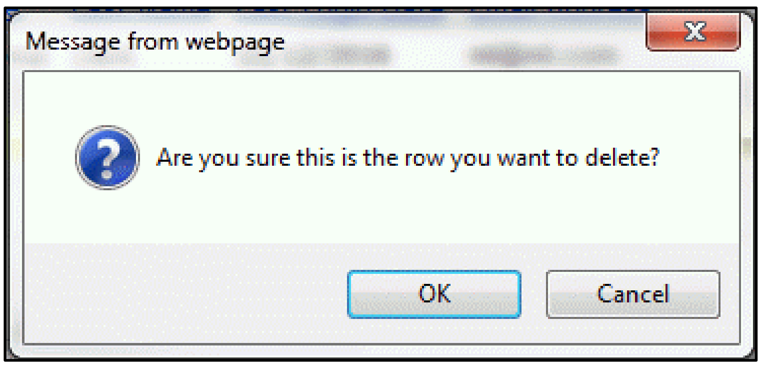


Figure 75 Dialog Box

2. Click **OK**. A confirmation message will be displayed at the top of the Clerk Maintenance Search page.

Figure 76 Confirmation Message

6.8 Clerk Account Log in for First Time

Clerk account users will be required to complete the steps for multi-factor authentication (MFA) when logging in for the first time and every 60 days thereafter.

With MFA, users are asked to provide two authentication methods to verify their identity when logging in to the Portal. MFA will protect Portal accounts against unauthorized access in case user login credentials are compromised.

MFA will be required to log in when a user changes any of the following account information:

- Account password
- Email address

When using MFA, a user will be sent a one-time code through their choice of email, text message (SMS), or phone call.

1. Access the Portal at https://www.forwardhealth.wi.gov/.

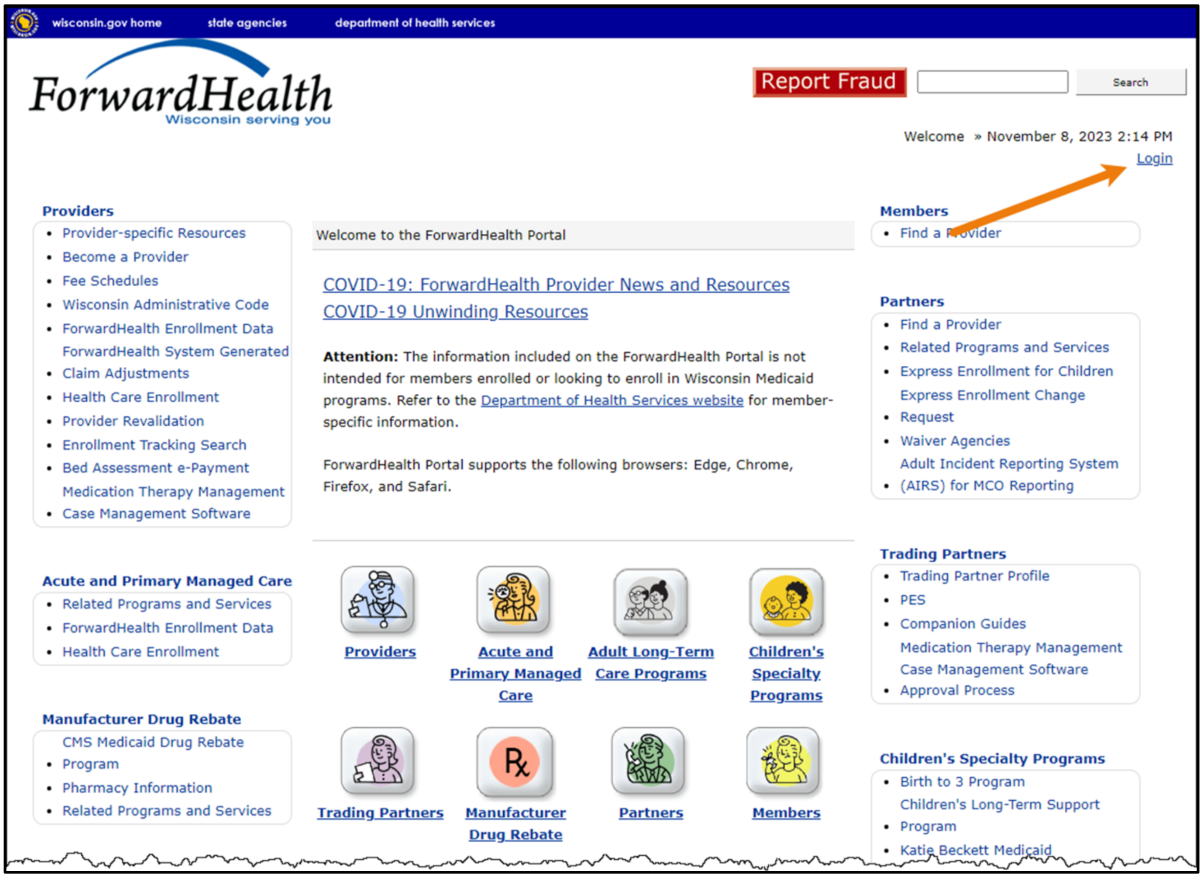


Figure 77 ForwardHealth Portal Page

2. Click **Login**. A Sign In box will be displayed.

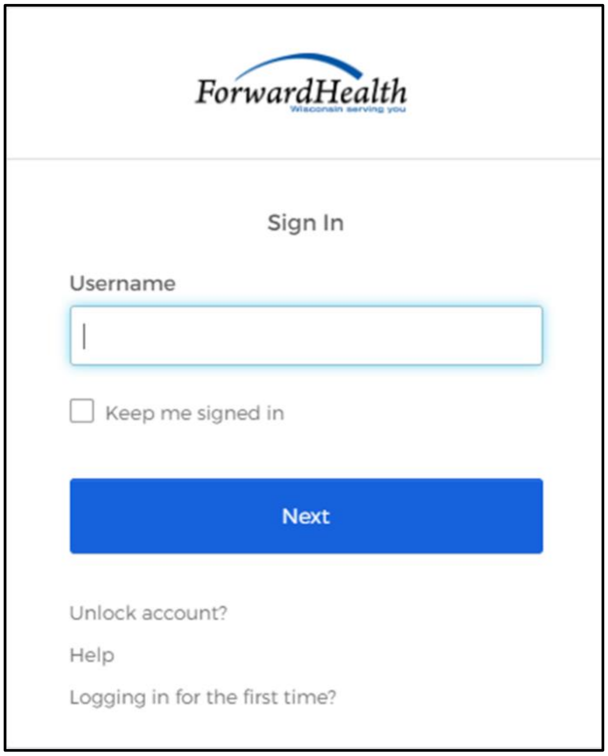


Figure 78 Sign In Box

3. Enter the user's username.
4. Click **Next**.

A Verify with your password box will be displayed.

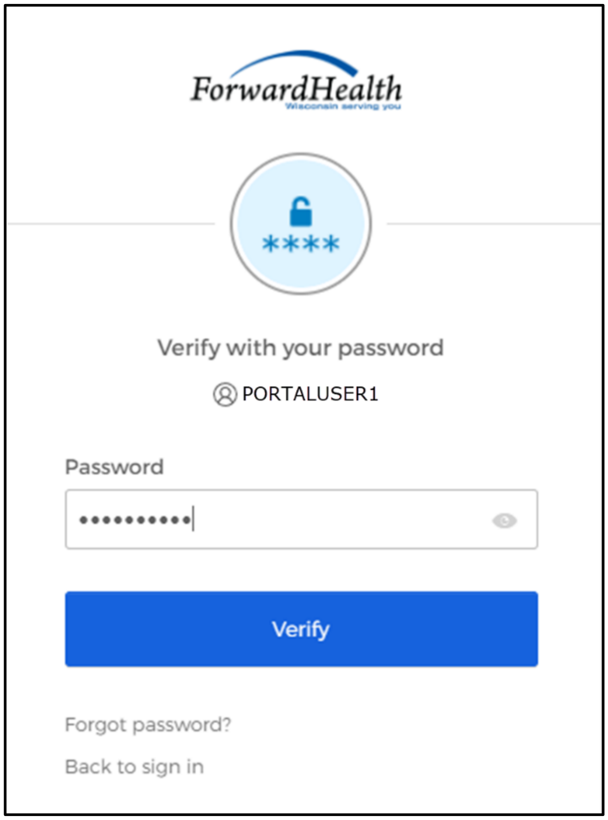


Figure 79 Verify With Your Password Box

5. Enter the user's password.
6. Click **Verify**.

A Get a verification email box will be displayed. Note: If the user's password expires when setting up MFA, a change password box will be displayed, and the user will be prompted to enter and re-enter their new password.

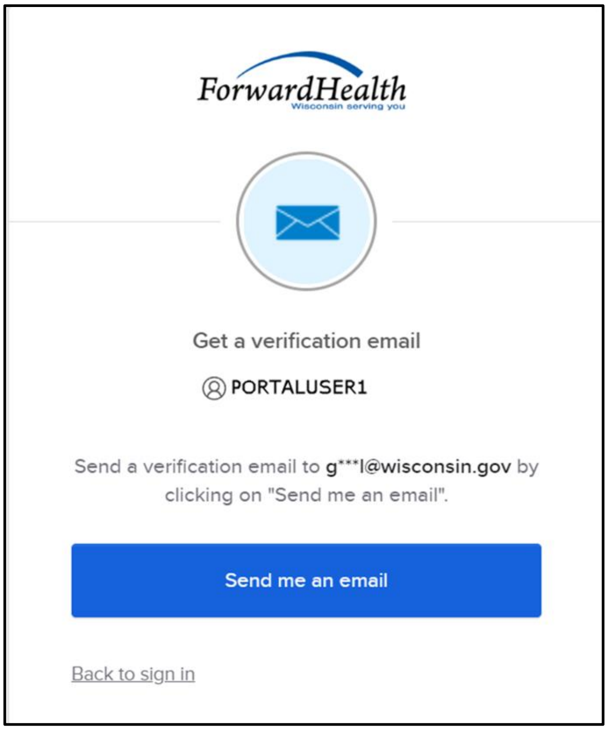


Figure 80 Get a Verification Email Box

7. Click **Send me an email**.

A box will be displayed indicating the email has been sent with a link to enter the code from the email.

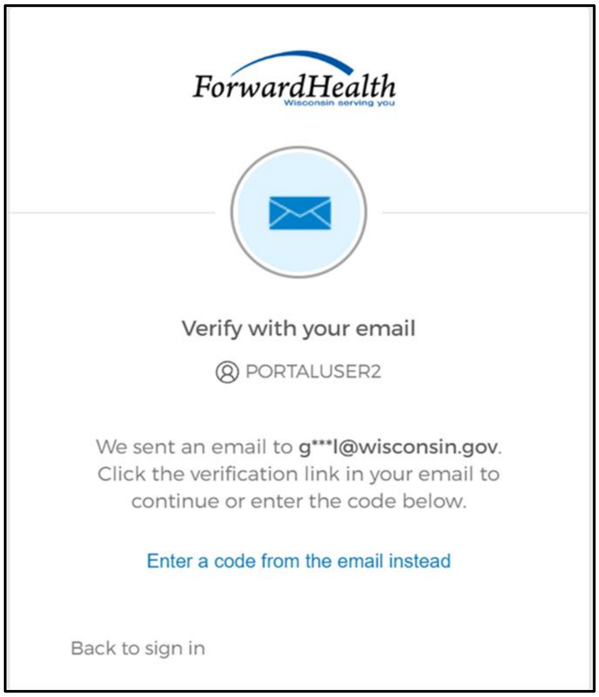


Figure 81 Verify With Your Email Box

8. The email sent to the user's email address includes a **Sign In** link (Option 1) and a verification code (Option 2).

Figure 82 One-Time Verification Code Email

9. The user can choose to either:
    - Click the **Sign In** link (Option 1) from the email.
    - Copy the verification code in the email (Option 2), return to the Verify with your email box, and click **Enter a verification code instead.** Enter the code from the email and click **Verify.**

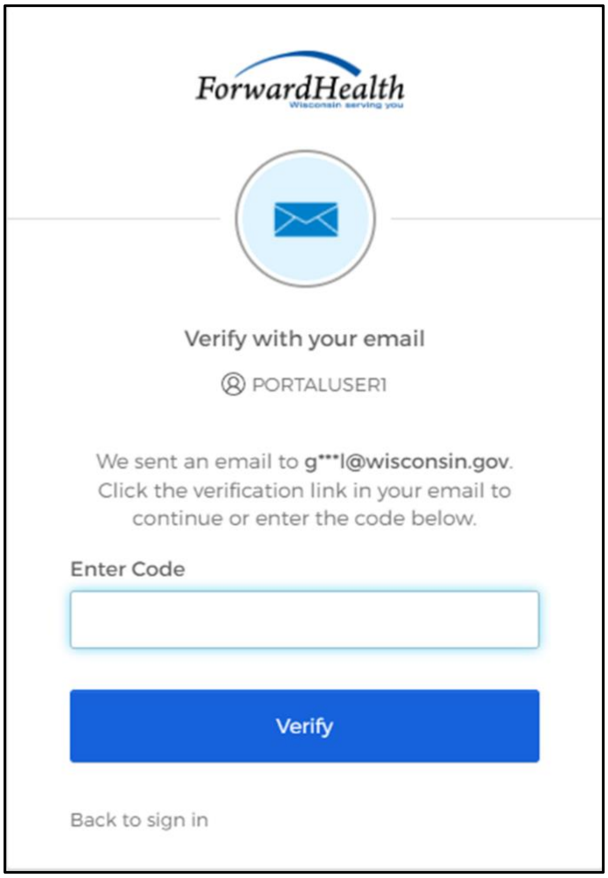


Figure 83 Verify With Your Email Box

A Set up security methods box will be displayed.

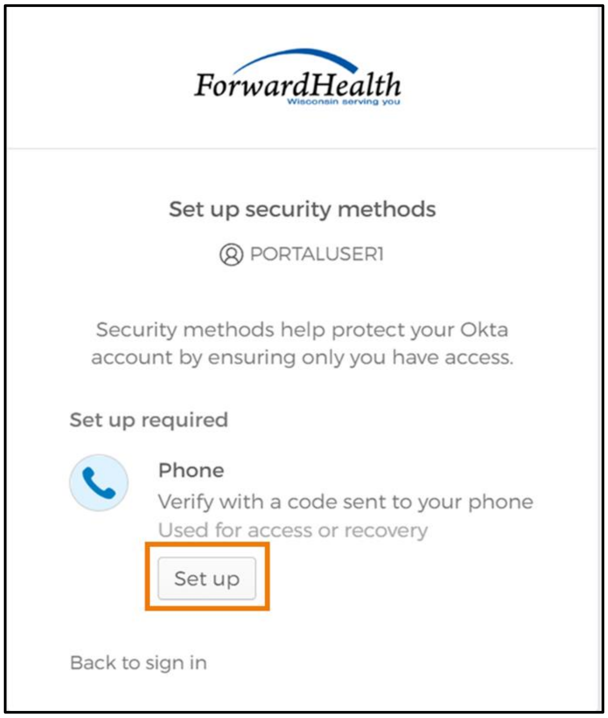


Figure 84 Set Up Security Methods Box

10. Click **Set up**.

A Set up phone authentication box will be displayed.

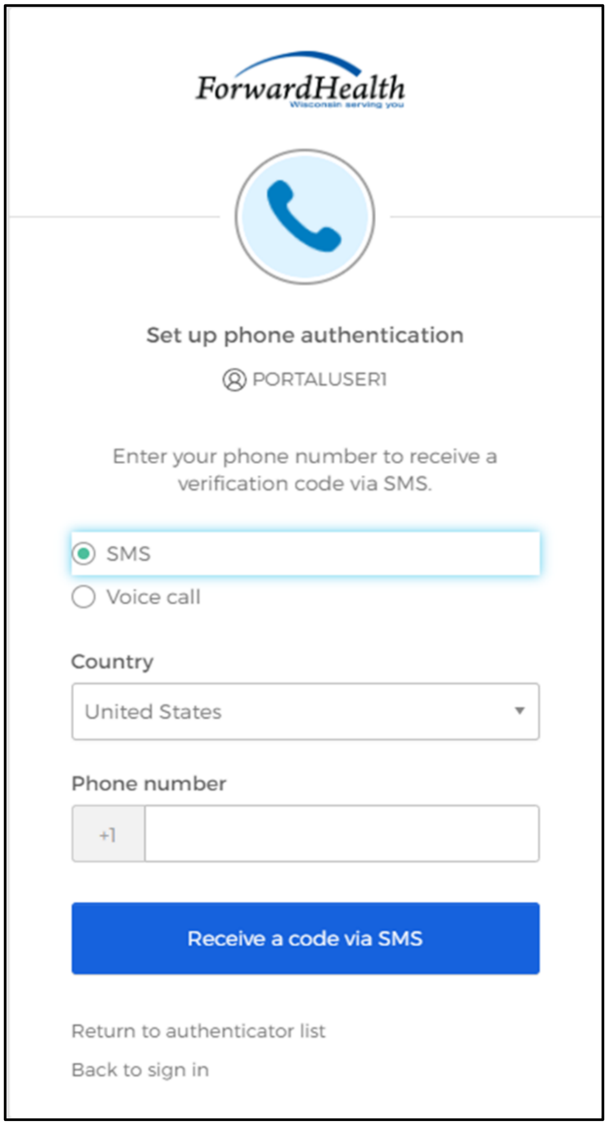


Figure 85 Set Up Phone Authentication Box

11. Select **SMS** (text) or **Voice call** for the phone authentication method.

12. Enter the phone number.

13. Click **Receive a code via SMS** or **Receive a code via voice call** depending on which option is selected.

A Set up phone authentication box will be displayed.

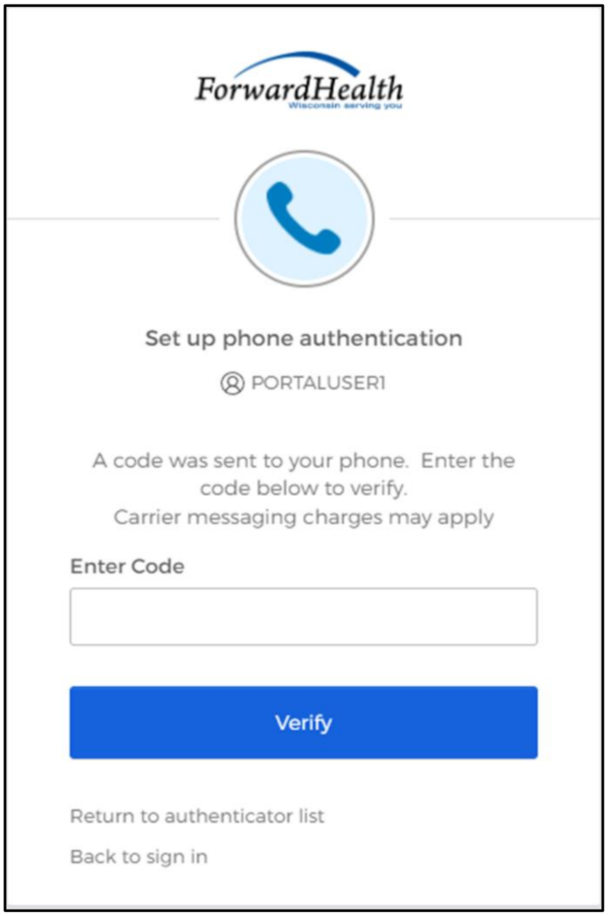


Figure 86 Set Up Phone Authentication Box

14. Enter the code that was sent via text or voice call in the **Enter Code** box.

15. Click **Verify**. MFA will be set up and the user will be signed in to the Portal.

7 Administrator Backup Information

Provider administrators are required to set up a backup contact for their Portal accounts via the Administrator Backup panel.

1. On the Account page, click **Administrator Backup Information**. The Administrator Backup panel will be displayed.

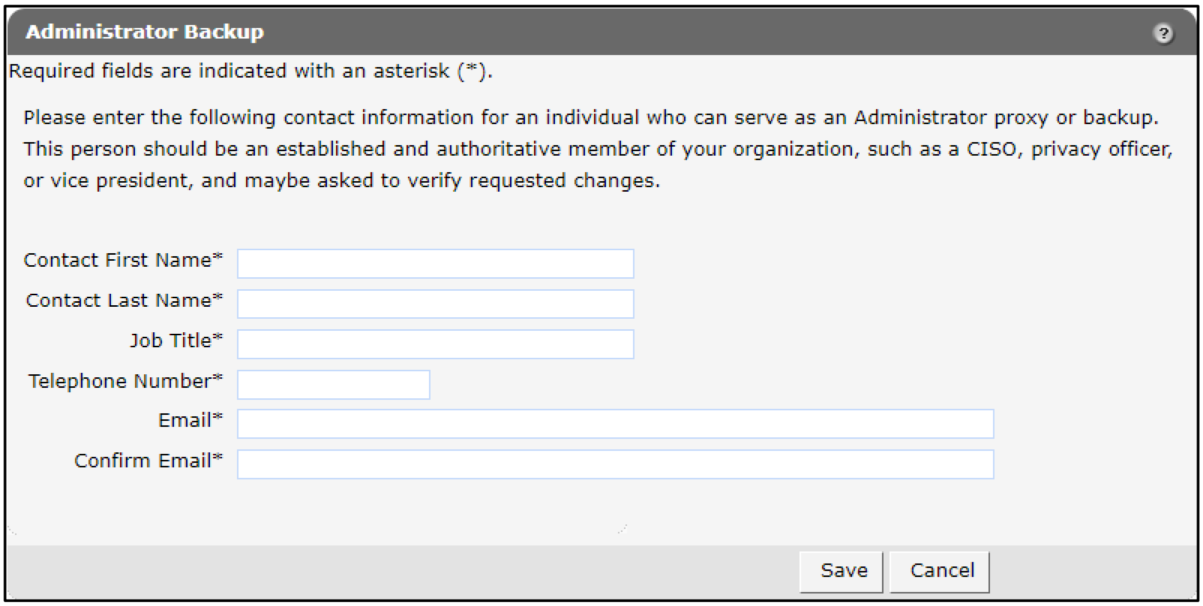


Figure 87 Administrator Backup Panel

2. Enter information for the backup contact in the fields. It is necessary to **complete all the fields** on this page.

   Note: The administrator backup email addresses cannot match those of the current administrator. Also, the phone number must include the area code. The number will be auto-formatted.

3. Click Save. A confirmation message will be displayed at the top of the page.

Figure 88 Confirmation Message

8 Clerk Last Logon

This function allows users with administrative accounts to search, identify, and remove inactive clerk accounts.

On the Account page, click **Clerk Last Logon**. The Clerk Last Logon panel will be displayed.

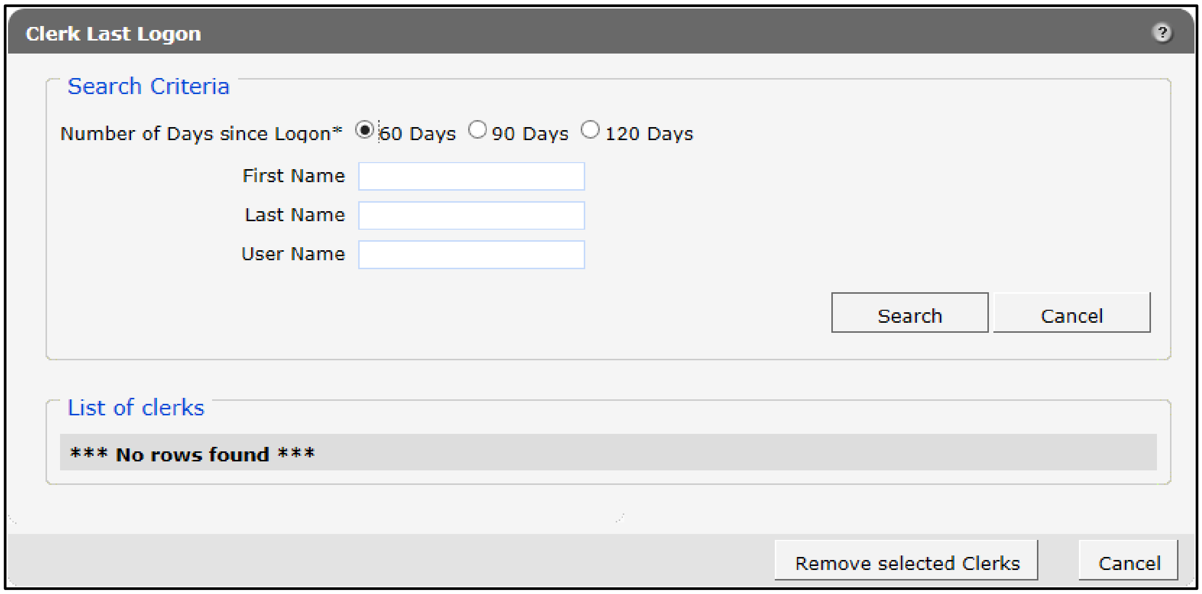


Figure 89 Clerk Maintenance Search Panel

Through the Clerk Last Logon panel, users with administrative accounts can search for users with inactive accounts and can also identify and remove clerks from a list of their organization's clerk accounts.

Note: Users with clerk administrative accounts may not administer their own accounts or other administrative or clerk administrative accounts.

8.1 Search and Remove a Clerk Account

The Clerk Last Logon panel allows a user to select an existing clerk within the provider organization based on the number of days since their last logon.

1. In the Search Criteria section, click the button indicating the number of days since the clerk's last logon. Options include periods of at least 60 days, 90 days, or 120 days from the clerk's last logon.

2. Enter any information for the clerk in any combination in the Search Criteria section. Alternatively, leave the First Name, Last Name, and User Name fields blank to bring up a list of all clerks associated with the provider organization based on the number of days since their last logon.

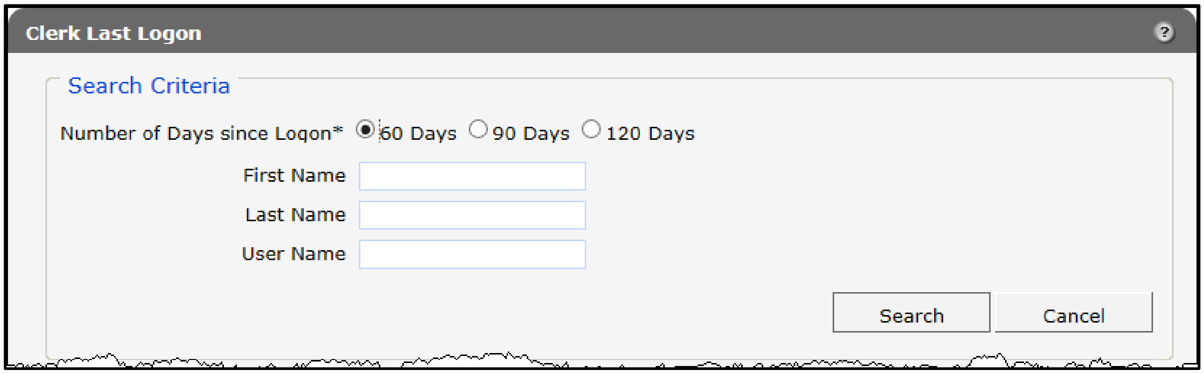


Figure 90 Search Criteria Section

3. Click **Search**. The clerk(s) will be listed under the "List of clerks" section.

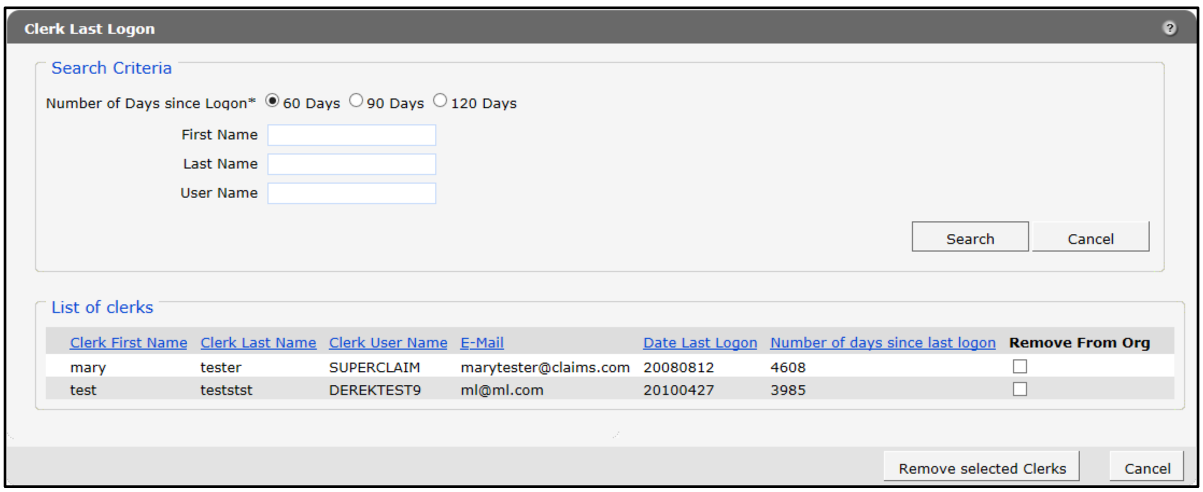


Figure 91 List of Clerks Section

4. Check the box under the Remove From Org column.

5. Click **Remove selected Clerks**. The selected clerks will be removed from the Portal.

   Note: The user can click **Cancel** to return to their secure account page.

9 Add Organization

The Add Organization function allows users with an administrative account to add multiple organizations to an existing Portal account. This feature offers the convenience of managing multiple organizations within one Provider Portal account as an alternative to creating separate Provider Portal accounts for each organization.

After adding an organization to an account, users with an administrative account are authorized to perform all tasks as defined by the roles available for that organization.

In addition, account users granted the necessary permissions may move from one organization to another through the Switch Organization function without having to log out of the account.

To add an organization to an account:

1. Follow the steps in Chapter 2 Request Portal Access of this guide to request a PIN.
2. Once the user has received the PIN letter, access the Portal at https://www.forwardhealth.wi.gov/.
3. Log in to the account to which the user wishes to add the new organization. The user's secure Provider page will be displayed.
4. Click **Account** on the main menu at the top of the page. The Account Home page will be displayed.
5. Click **Add Organization**. The Add Organization page will be displayed.

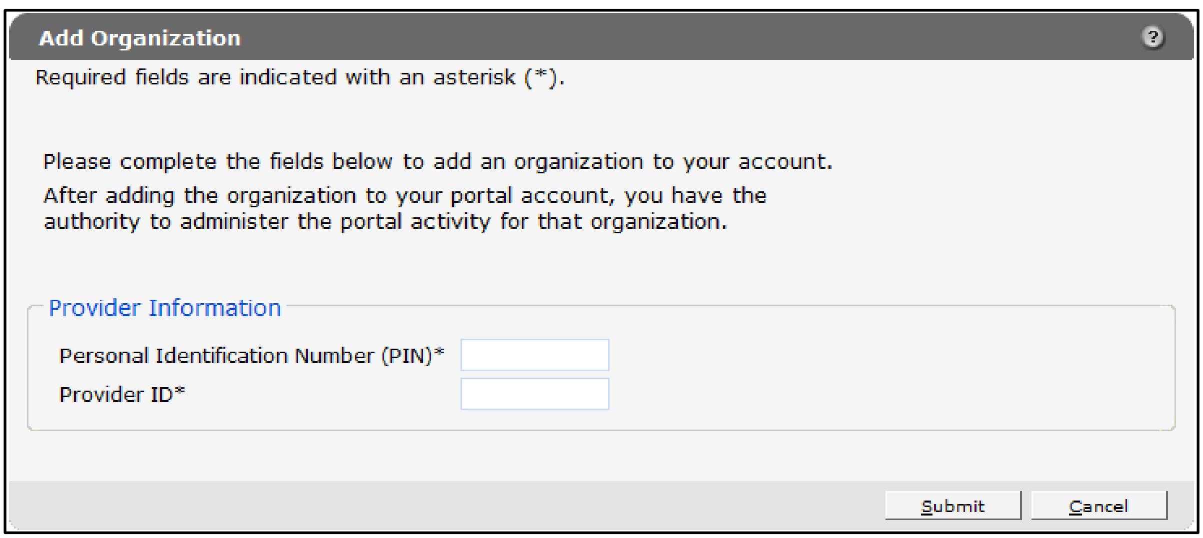


Figure 92 Add Organization Page

6. Enter the PIN sent to the organization in the PIN letter.

Note: Each organization needs to request and receive a PIN in order to be added to an existing Portal account. After receiving a PIN, users should follow the steps for adding an organization to an existing account instead of the steps outlined in Chapter 3 Set Up an Account of this guide.

7. Enter the provider's NPI or the Medicaid Provider ID in the Provider ID field.

8. Click **Submit**. A confirmation message will be displayed at the top of the page.

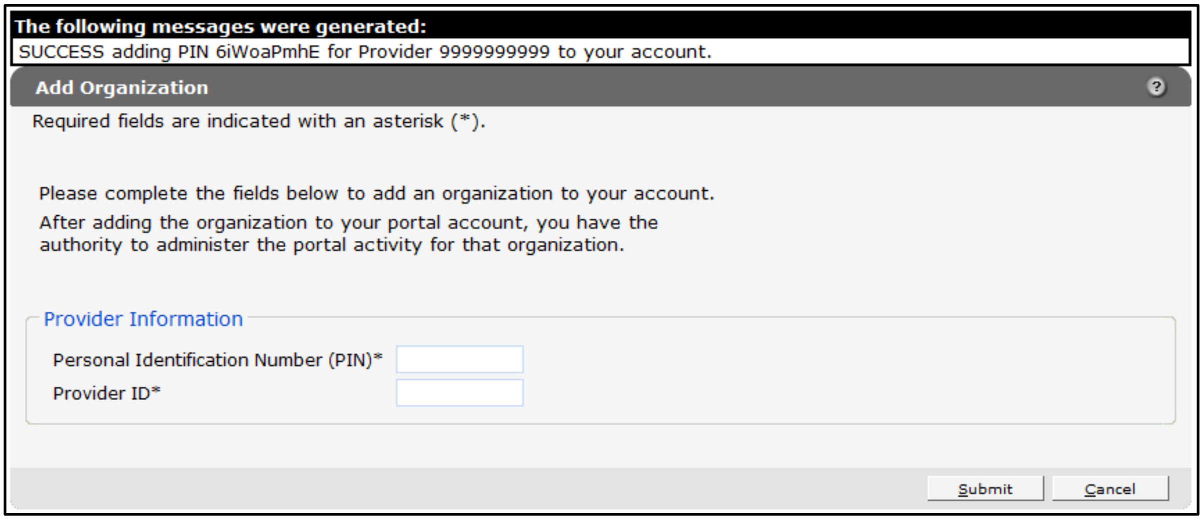


Figure 93 Add Organization Page With Confirmation Message

If the user receives an error message, correct the error(s) and click **Submit** again.

Once the organization is added to the Portal account, the user will be able to return to the Account Home page to switch to and perform tasks for the new organization's account.

Note: If an administrative account has a new organization added to it, clerks set up under the initial organization are not automatically linked to the new organization. Clerk administrative and clerk accounts need to be added to the new organization via the Clerk Maintenance function. For more information, refer to Section 6.1 Add a Clerk of this guide.

9. Click **Account** on the main menu at the top of the page to return to the Account Home page. A dialog box will be displayed.

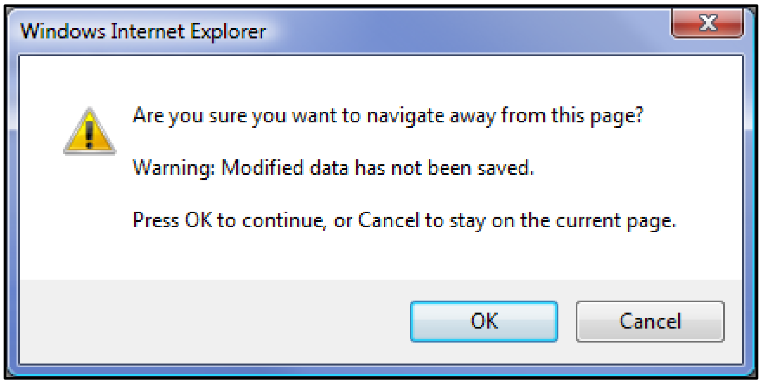


Figure 94 Dialog Box

10. Click **OK**. The Account Home page will be displayed.

11. For information about switching to the added organization, refer to Chapter 10 Switch Organization of this guide.

10 Switch Organization

Under the Switch Organization function:

- Users with administrative and clerk administrative accounts may assign roles to a clerk for a different organization within the same account without logging off.
- Clerks may perform tasks on behalf of multiple organizations within the same account without logging off.
- Users may change their default login organization.

10.1 Search and Switch to Organization

1. On the Account Home page, click Switch Organization. The switch organization page will be displayed.

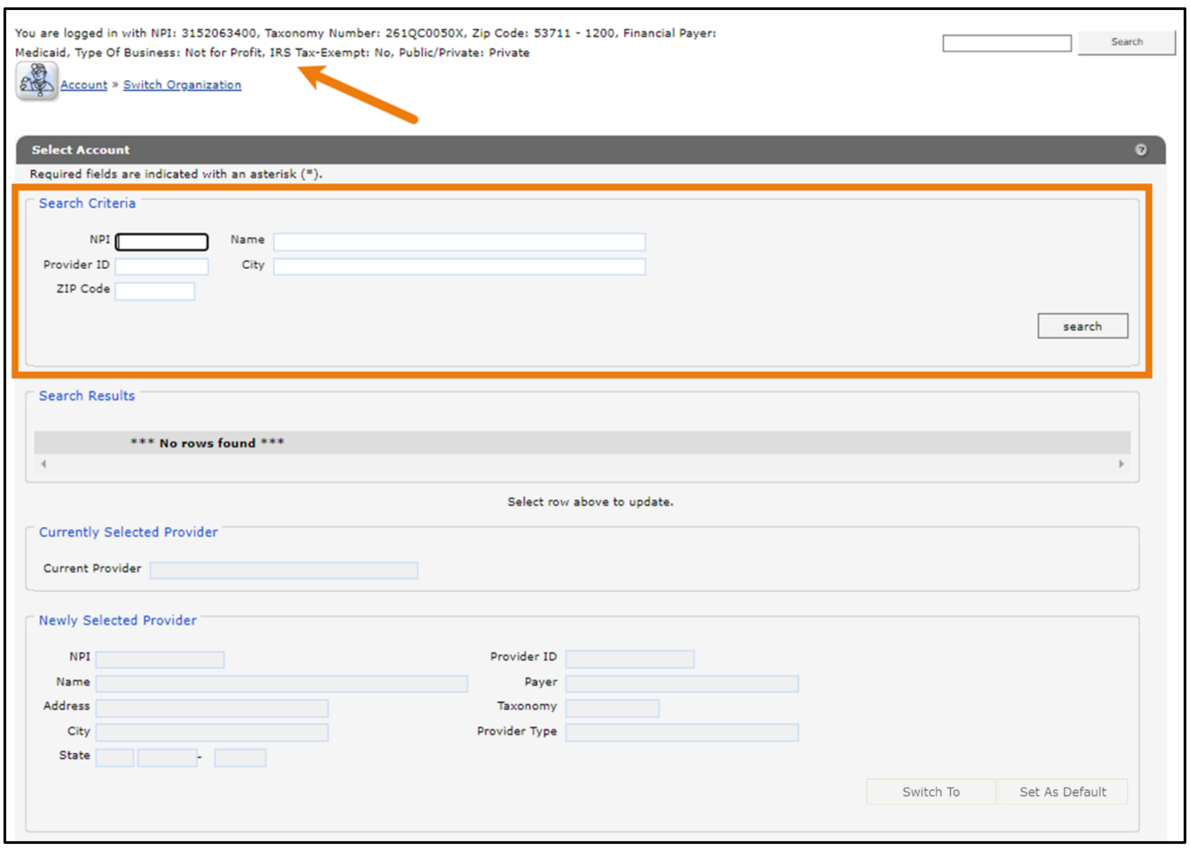


Figure 95 Switch Organization Page

The NPI or Provider ID that the user is currently logged in under will be displayed at the top of the page.

2. Enter any of the following search criteria for the organization in any combination in the “Search Criteria” section.
    - NPI
    - Provider ID
    - ZIP Code
    - Name
    - City
3. Click **search**. The organization(s) will be listed under the “Search Results” section.

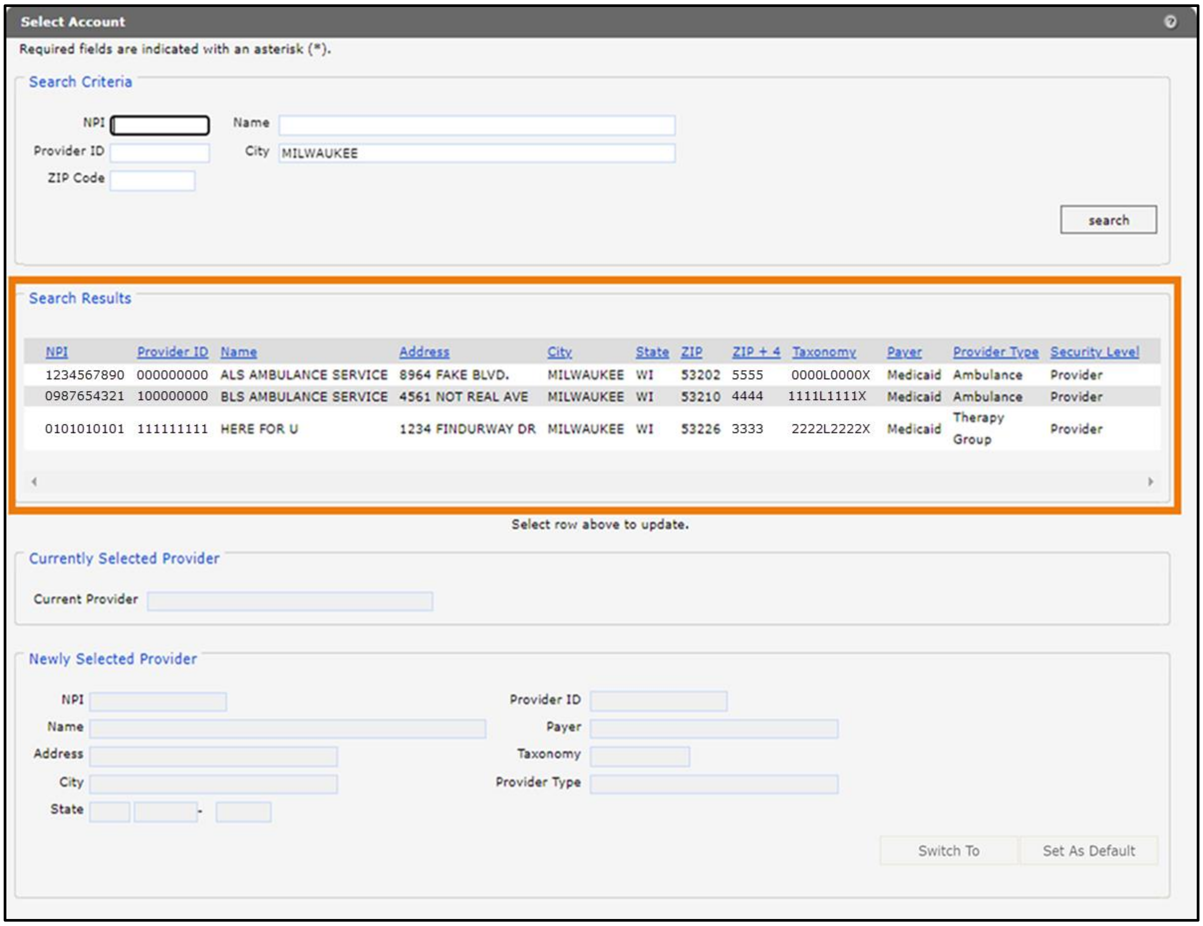


Figure 96 Switch Organization Page–Search Results

4. Click on the row containing the applicable organization. The organization's information will auto-populate in the "Currently Selected Provider" and "Newly Selected Provider" sections. Note: If only one organization is listed under the "Search Results" section the "Newly Selected Provider" section will auto-populate with the organization's information.

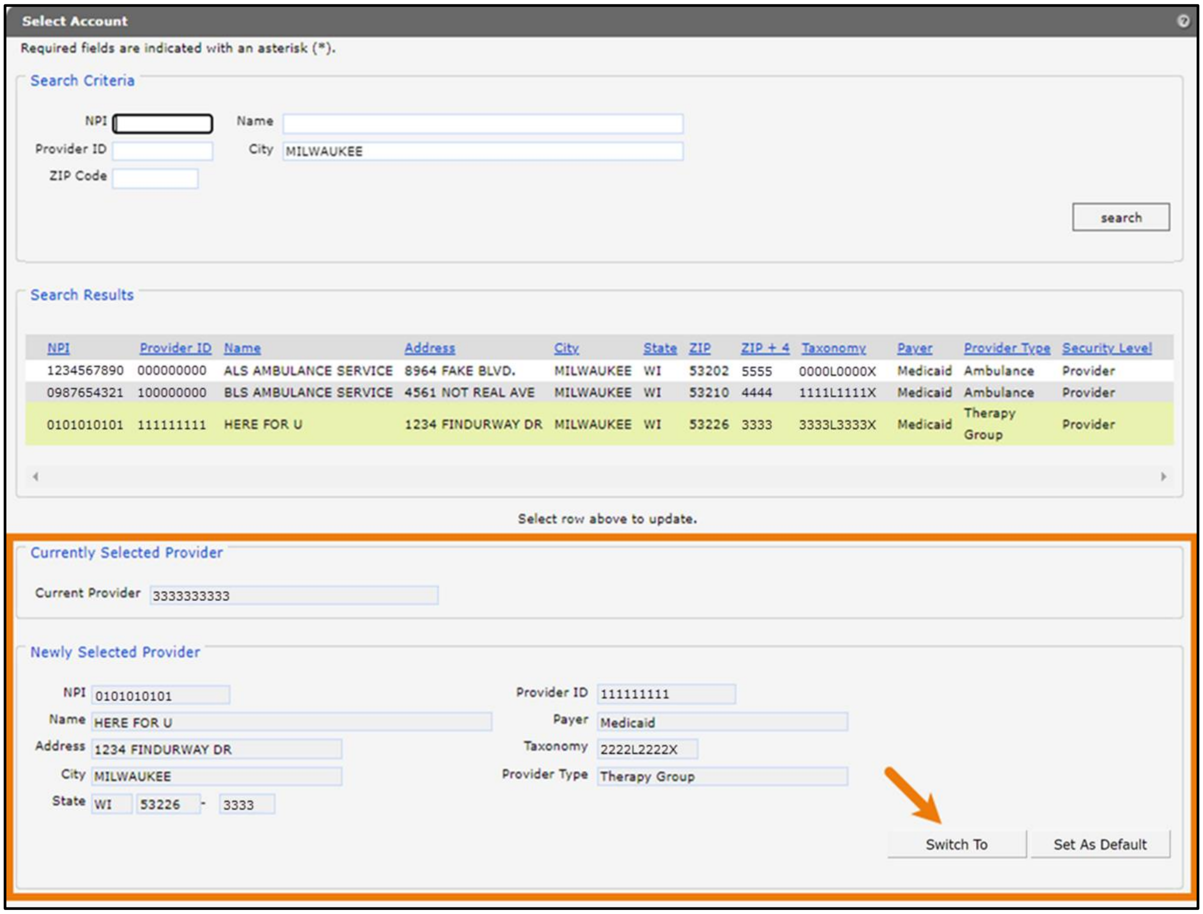


Figure 97 Switch Organization Page–Search Results Populated

5. If the user wishes to switch to the selected organization's account, click **Switch To**.

6. The user will be returned to the secure Provider page. The NPI to which they switched will be displayed at the top of the page.

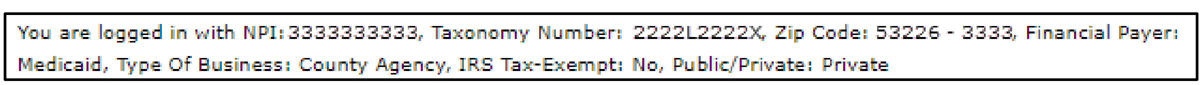


Figure 98 Log In Information

10.2 Set As Default Login Organization

1. To make an organization the default login user, on the Switch Organization page, click the row of the desired organization. The organization's information will auto-populate in the "Currently Selected Provider" and "Newly Selected Provider" sections.

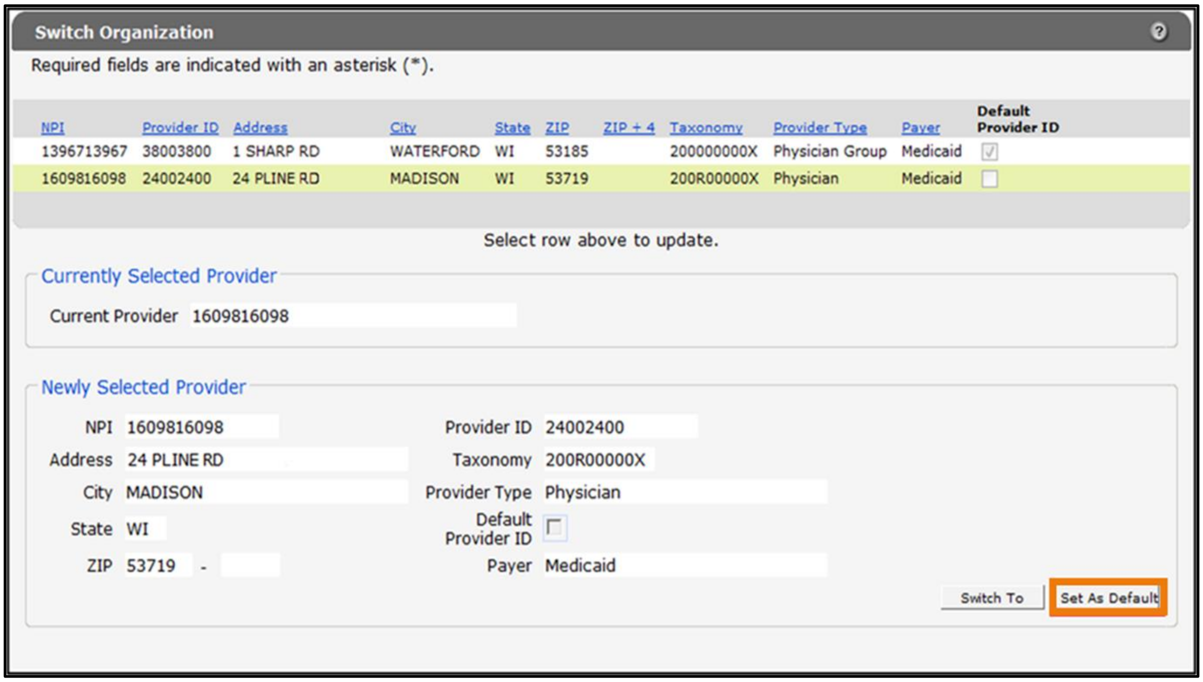


Figure 99 Switch Organization Page With Auto-Populated Information

2. Click **Set As Default**. The Switch Organization page will refresh and check marks will be displayed in the Default Provider ID boxes for the selected organization.

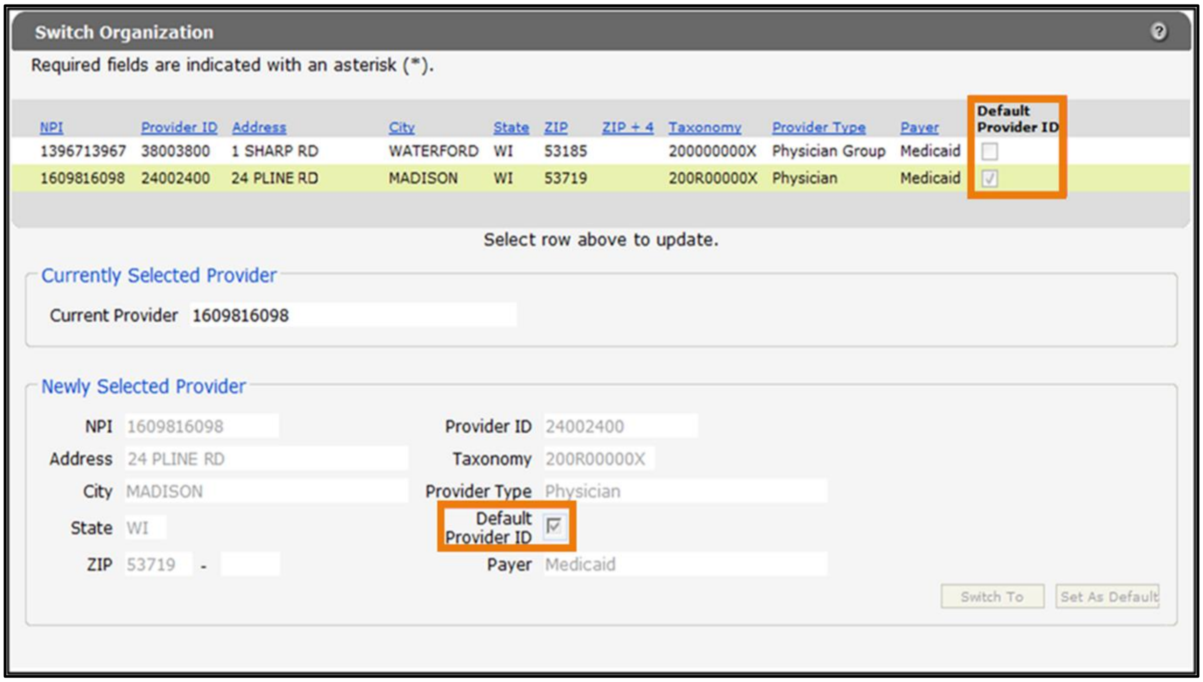


Figure 100 Switch Organization Page

The selected organization will automatically be the user each time they log in to their account.

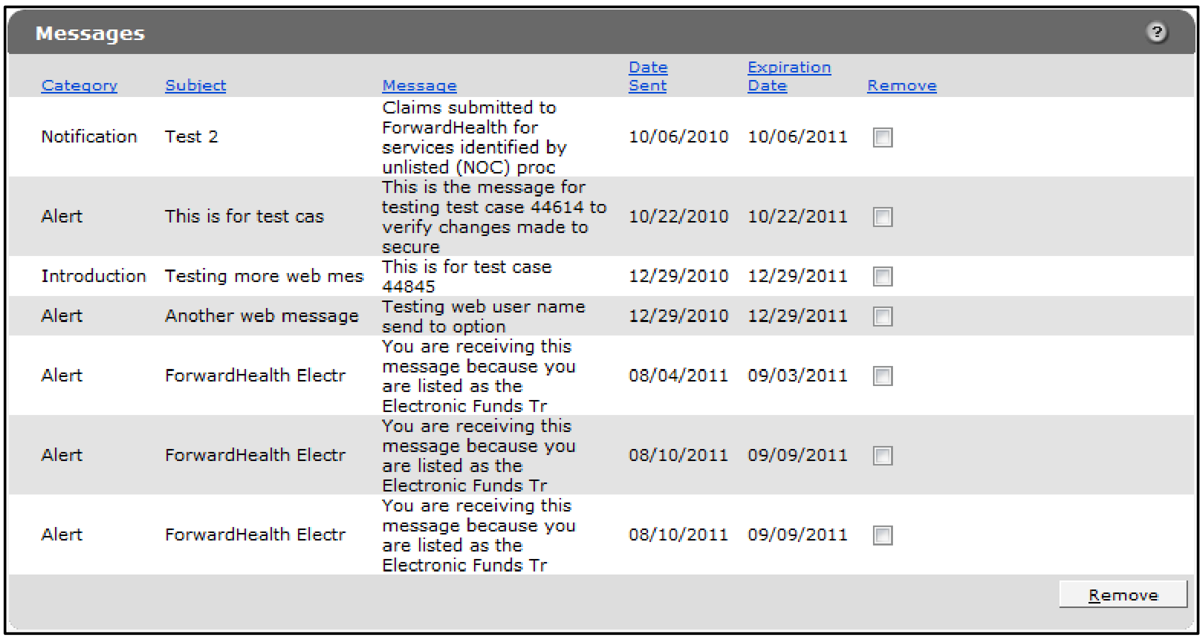
11 Messages

The Messages page acts as a one-way message center for providers to receive electronic notifications and provider publications from ForwardHealth. The most recent messages are also displayed on the user's secure Provider page.

Messages are sent to the user's account by ForwardHealth and are available from the date sent to the expiration date. A message is removed from the Messages page if the user manually removes it or if it is automatically removed on the expiration date set by ForwardHealth.

1. On the Account Home page, click **Messages**. The Messages page will be displayed.

   Note: If there is only one message, the message and "Message" section will be displayed.



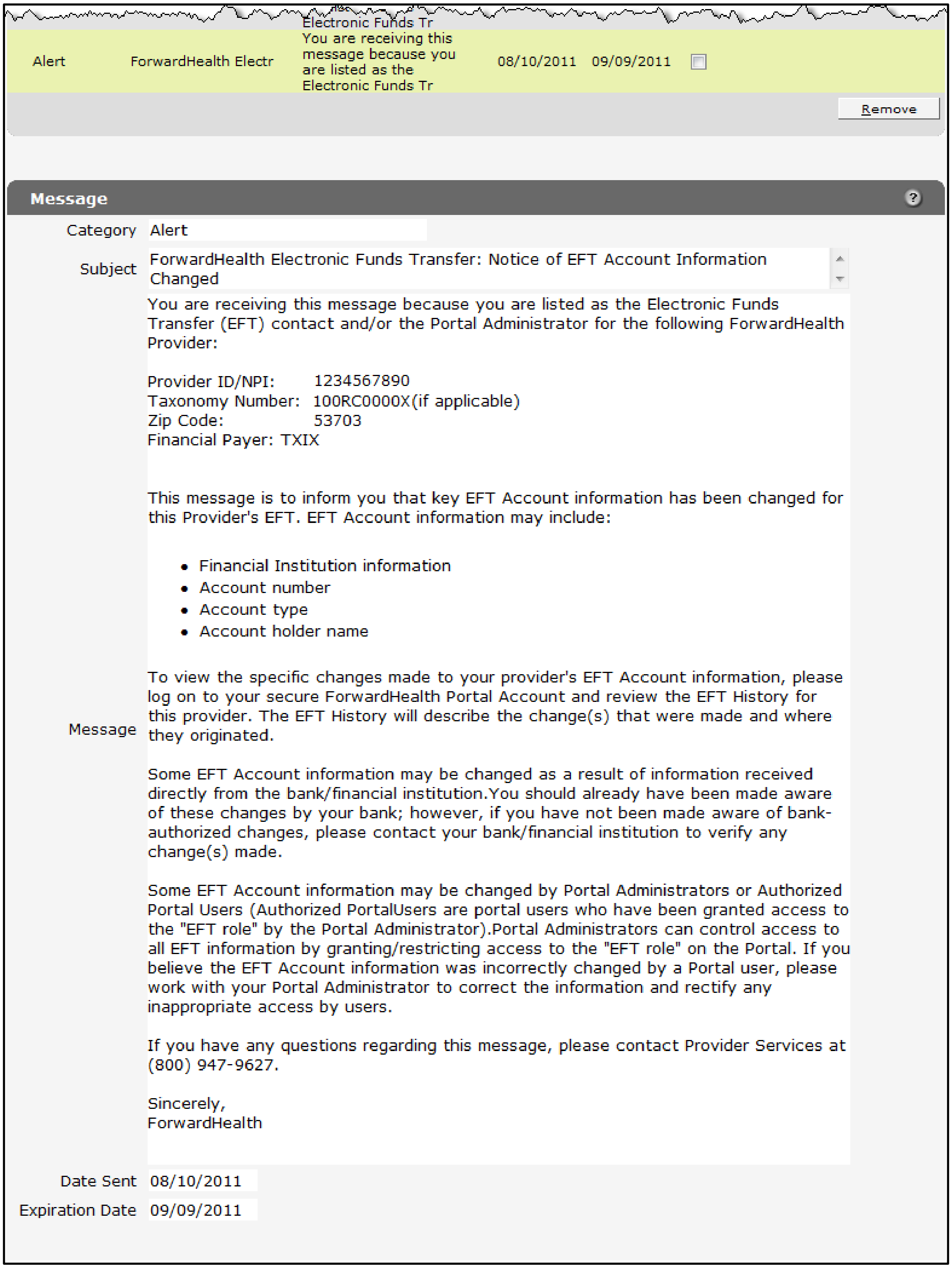
Messages

Category	Subject	Message	Date Sent	Expiration Date	Remove
Notification	Test 2	Claims submitted to ForwardHealth for services identified by unlisted (NOC) proc	10/06/2010	10/06/2011	
Alert	This is for test cas	This is the message for testing test case 44614 to verify changes made to secure	10/22/2010	10/22/2011	
Introduction	Testing more web mes	This is for test case 44845	12/29/2010	12/29/2011	
Alert	Another web message	Testing web user name send to option	12/29/2010	12/29/2011	
Alert	ForwardHealth Electr	You are receiving this message because you are listed as the Electronic Funds Tr	08/04/2011	09/03/2011	
Alert	ForwardHealth Electr	You are receiving this message because you are listed as the Electronic Funds Tr	08/10/2011	09/09/2011	
Alert	ForwardHealth Electr	You are receiving this message because you are listed as the Electronic Funds Tr	08/10/2011	09/09/2011	

Remove

Figure 101 Messages Page

2. Click the applicable message. The "Message" section will be displayed at the bottom of the page.



Alert	ForwardHealth Electr	Electronic Funds Tr You are receiving this message because you are listed as the Electronic Funds Tr	08/10/2011	09/09/2011	

Remove

Message

Category: Alert

Subject: ForwardHealth Electronic Funds Transfer: Notice of EFT Account Information Changed

Message:

You are receiving this message because you are listed as the Electronic Funds Transfer (EFT) contact and/or the Portal Administrator for the following ForwardHealth Provider:

Provider ID/NPI: 1234567890
Taxonomy Number: 100RC0000X(if applicable)
Zip Code: 53703
Financial Payer: TXIX

This message is to inform you that key EFT Account information has been changed for this Provider's EFT. EFT Account information may include:

- Financial Institution information
- Account number
- Account type
- Account holder name

To view the specific changes made to your provider's EFT Account information, please log on to your secure ForwardHealth Portal Account and review the EFT History for this provider. The EFT History will describe the change(s) that were made and where they originated.

Some EFT Account information may be changed as a result of information received directly from the bank/financial institution.You should already have been made aware of these changes by your bank; however, if you have not been made aware of bank-authorized changes, please contact your bank/financial institution to verify any change(s) made.

Some EFT Account information may be changed by Portal Administrators or Authorized Portal Users (Authorized PortalUsers are portal users who have been granted access to the "EFT role" by the Portal Administrator).Portal Administrators can control access to all EFT information by granting/restricting access to the "EFT role" on the Portal. If you believe the EFT Account information was incorrectly changed by a Portal user, please work with your Portal Administrator to correct the information and rectify any inappropriate access by users.

If you have any questions regarding this message, please contact Provider Services at (800) 947-9627.

Sincerely,
ForwardHealth

Date Sent: 08/10/2011

Expiration Date: 09/09/2011

Figure 102 Message Section

To delete a message:

1. Check the Remove box next to the message.

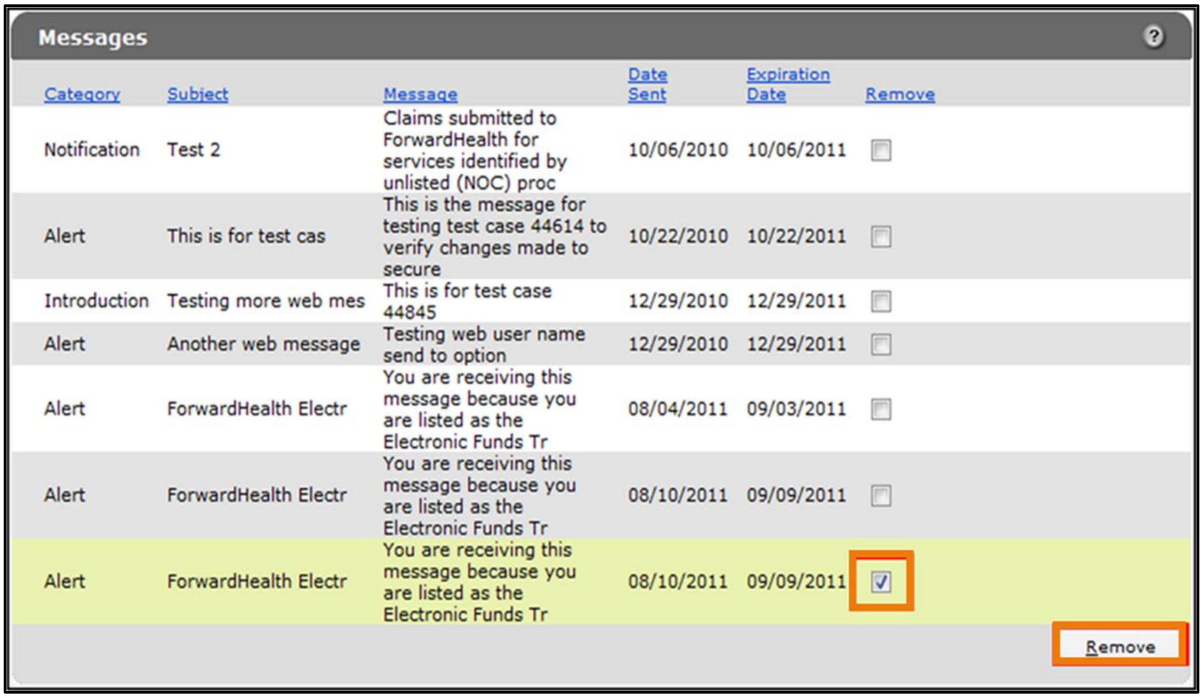


Figure 103 Messages Page

2. Click **Remove**. The message will be deleted from the Messages page.

12 Message Center

The message center function allows users to have a dialogue with Wisconsin Department of Health Services staff without leaving the Portal. Messages can be exchanged on a variety of topics along with the ability to attach documentation that needs to be included in the conversation.

1. On the secure Portal page, click **Message Center**. The Message Center panel will be displayed. Each view includes the same functionality (for example, read, reply, print) described below.

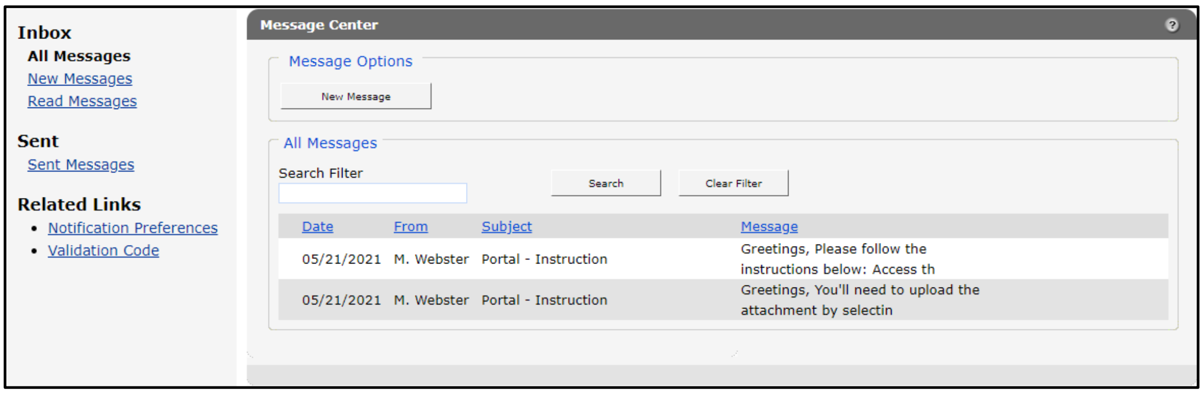


Figure 104 Message Center Panel

12.1 Send a New Message

1. Click **New Message**. The "Message," "Upload Attachment," and "Attachments" sections will be displayed on the Message Center panel.

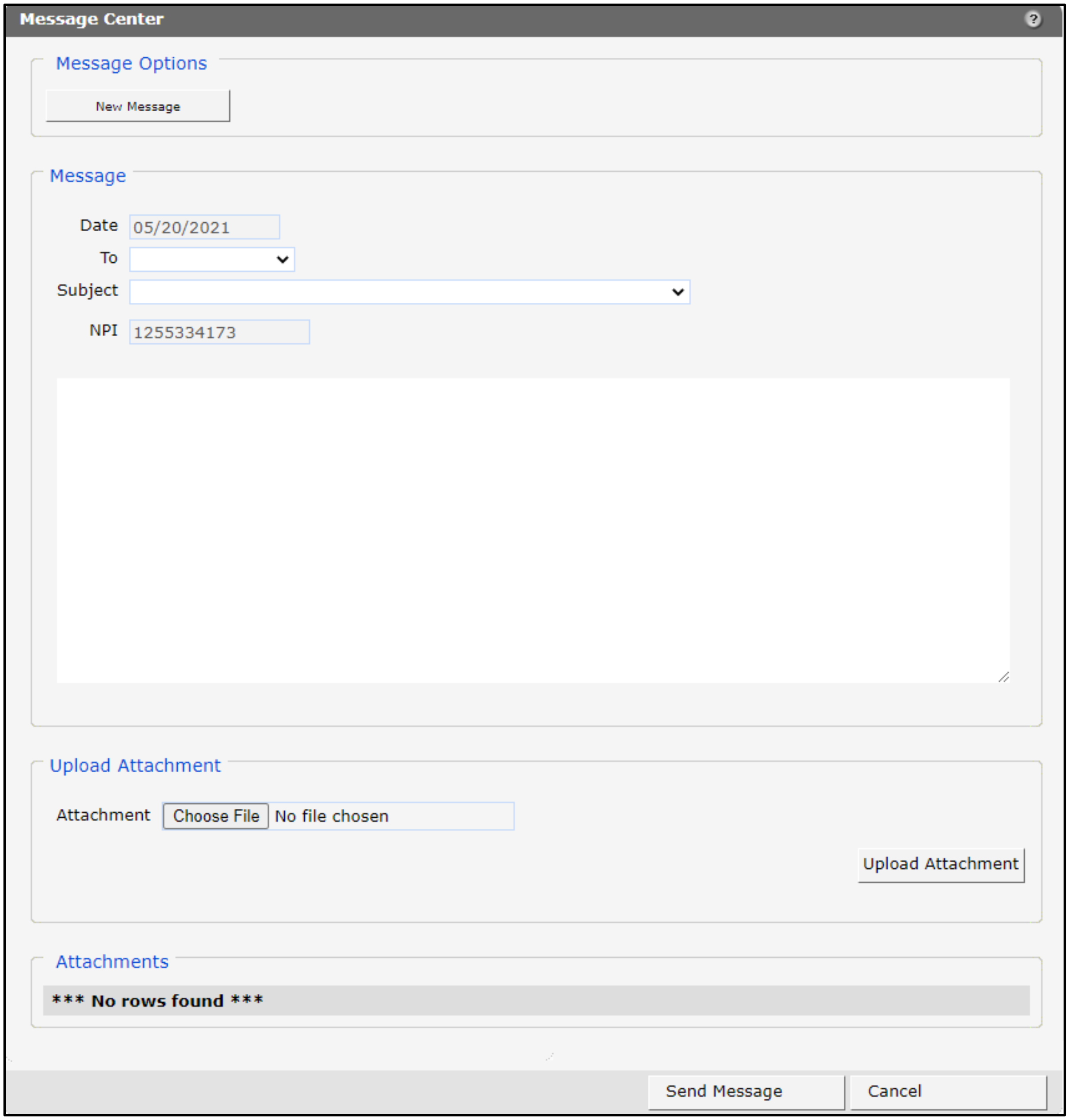


Figure 105 Message Center Panel for New Message

2. Select the message recipient from the drop-down menu in the *To* field.

   Note: The options in the drop-down menu will differ based on the user's security role.

3. Select a message subject from the drop-down menu.

4. Enter a message in the free text space. Messages are limited to 4,000 characters.

5. Click **Choose File** under the “Upload Attachment” section to upload an attachment for the message.

6. Select the desired file and double-click. The file name will appear after the **Choose File** box.

7. Click **Upload Attachment**. A confirmation message will be displayed at the top of the page and the file name will appear under the “Attachments” section.

Figure 106 File Upload Confirmation Message

The following file extensions may be uploaded: .jpg, .png, .csv, .pdf, .jpeg, and .xlsx.

8. Click **Send Message**. A confirmation message will be displayed at the top of the page.

Figure 107 Message Sent Confirmation Message

12.2 Read a Message

1. Click the row of the desired message at the bottom of the All Messages, New Messages, Read Messages, or Sent Messages views. The Message Center panel will be displayed with message details and options.

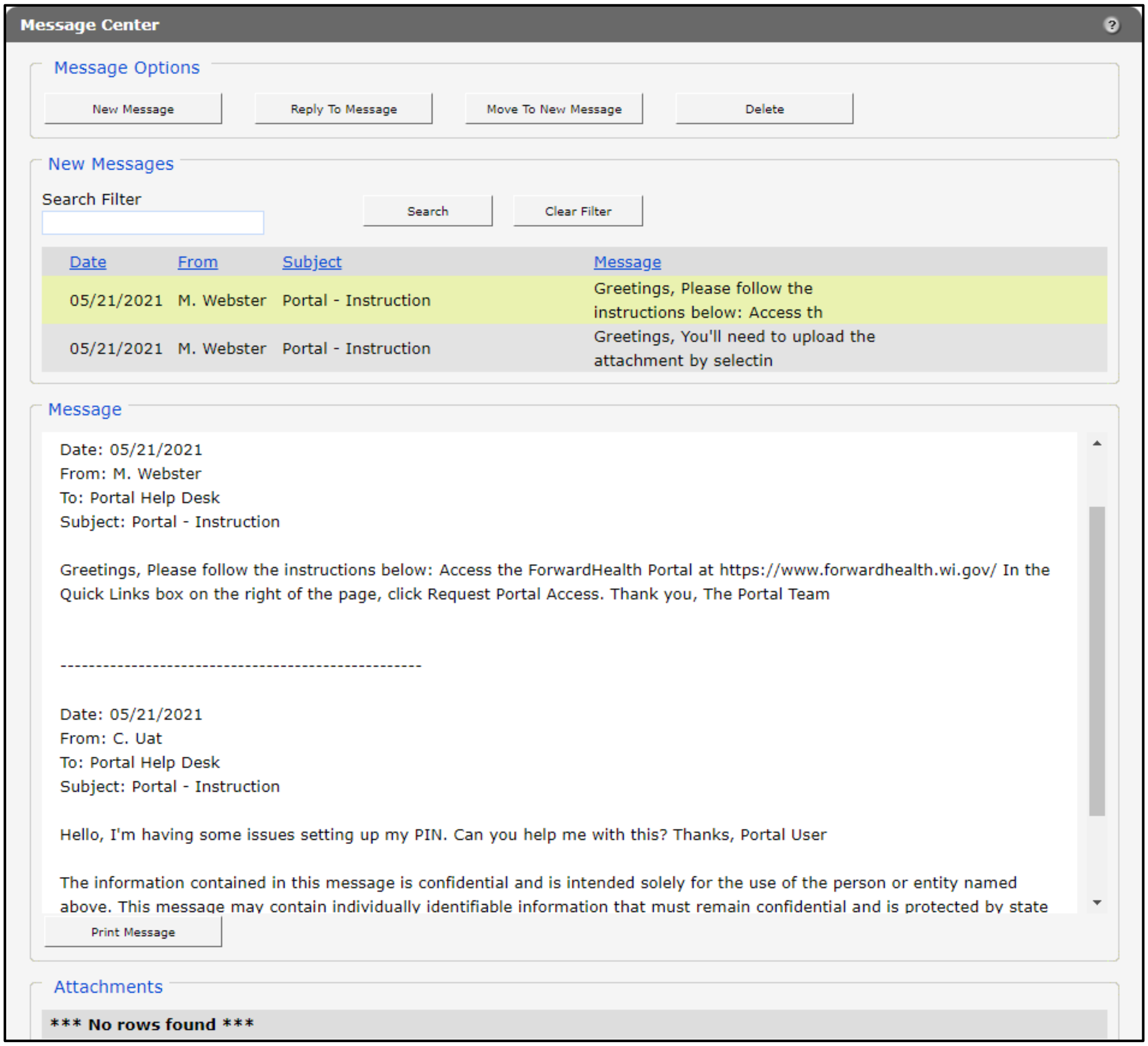


Figure 108 Message Center Panel for Reading Messages

2. If desired, click Print Message to open a printable view of the message. Select the print icon at the bottom of the page to choose the appropriate printer and properties.
3. The user can choose to move messages from the “All Messages” or “Read Messages” sections to the “New Messages” section by clicking **Move to New Message**. A confirmation message will be displayed at the top of the page.

Figure 109 Message Moved Confirmation Message

12.2.1 Respond to an Open Message

1. Click **Reply to Message** to respond to an inbox message. A message reply panel will be displayed.

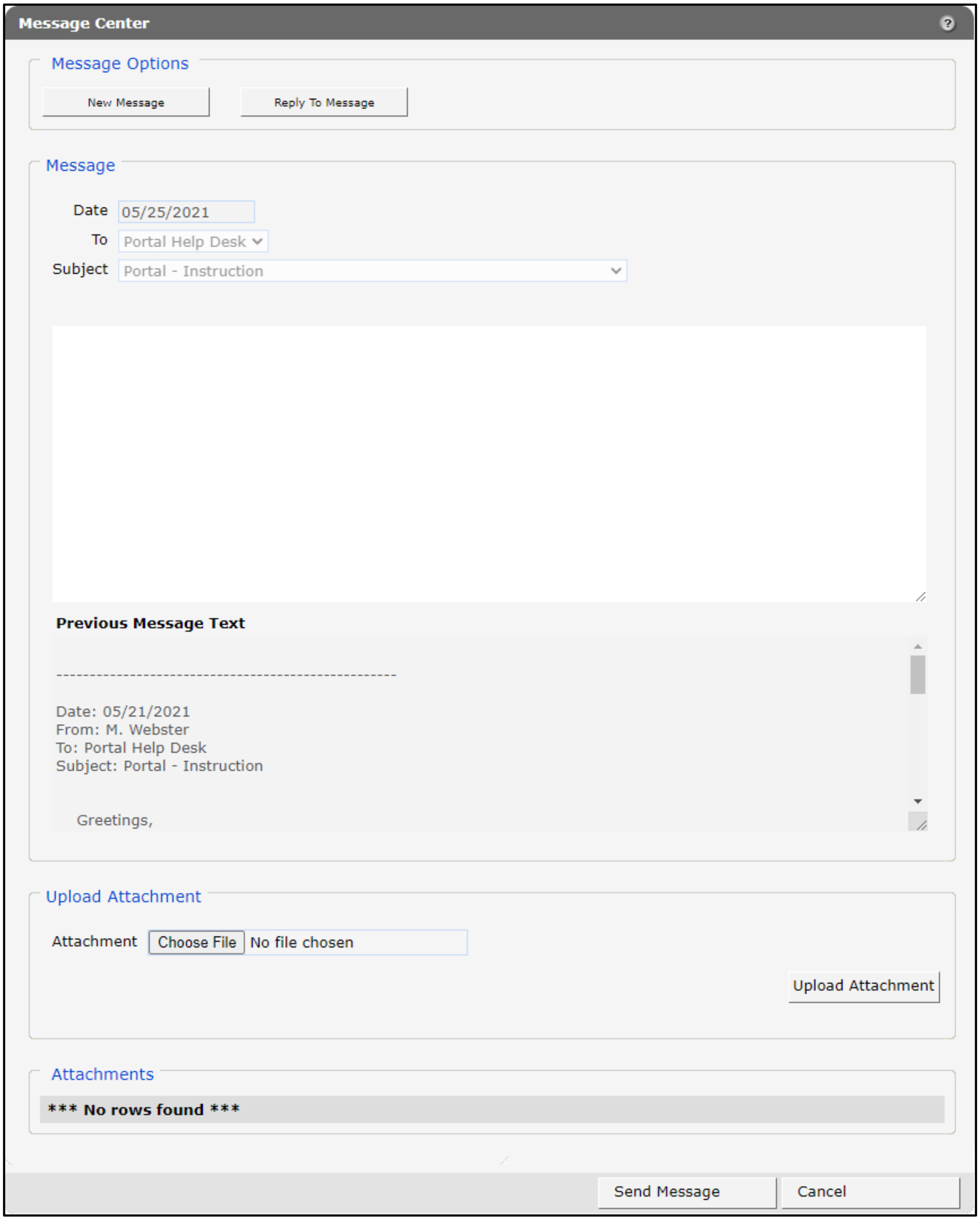


Figure 110 Message Center Panel for Replying to Messages

2. Enter the message text in the free text space. Messages are limited to 4,000 characters.
3. Click **Choose File** under the "Upload Attachment" section to upload an attachment for the message.
4. Select the desired file and double-click. The file name will appear after the **Choose File** box.
5. Click **Upload Attachment**. A confirmation message will be displayed at the top of the page and the file name will appear under the Attachments section.

Figure 111 File Upload Confirmation Message

The following file extensions are allowed for uploading: .jpg, .png, .csv, .pdf, .jpeg, and .xlsx.

6. Click **Send Message**. A confirmation message will be displayed at the top of the page.

Figure 112 Message Sent Confirmation Message

12.3 Search for a Message

1. Enter a keyword in the Search Filter field on the All Messages, New Messages, Read Messages, or Sent Messages views.
2. Click **Search**. Messages containing the keyword will be displayed.

   If the desired message is not found, click **Clear Filter**, enter a new keyword, and click **Search.**

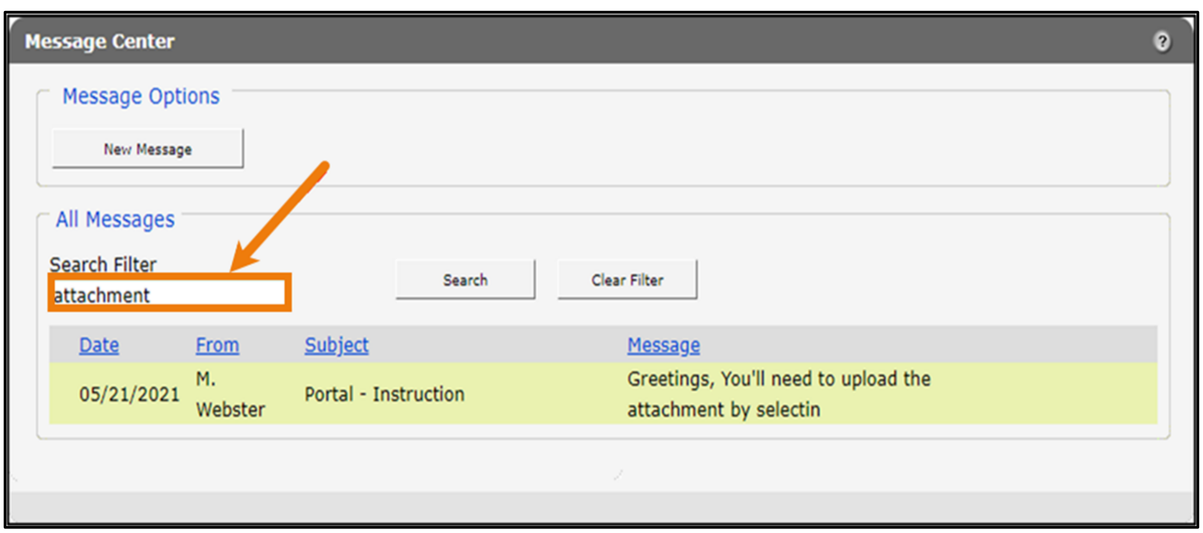


Figure 113 Message Center Search Filter

3. Click the row in the search results to open the message.

12.4 Notification Preferences and Validation Code

Users can sign up to receive notifications of Portal messages through email, text, or both. After signing up, a verification email will be sent to the user to register their device.

1. On the Message Center page, click **Notification Preferences** under Related Links. The Notifications Preferences panel will be displayed. The “Notification Preferences,” “Register Email,” “Register Mobile Number,” and “Mobile Notifications – Terms and Conditions” sections will be displayed on the Notification Preferences panel.

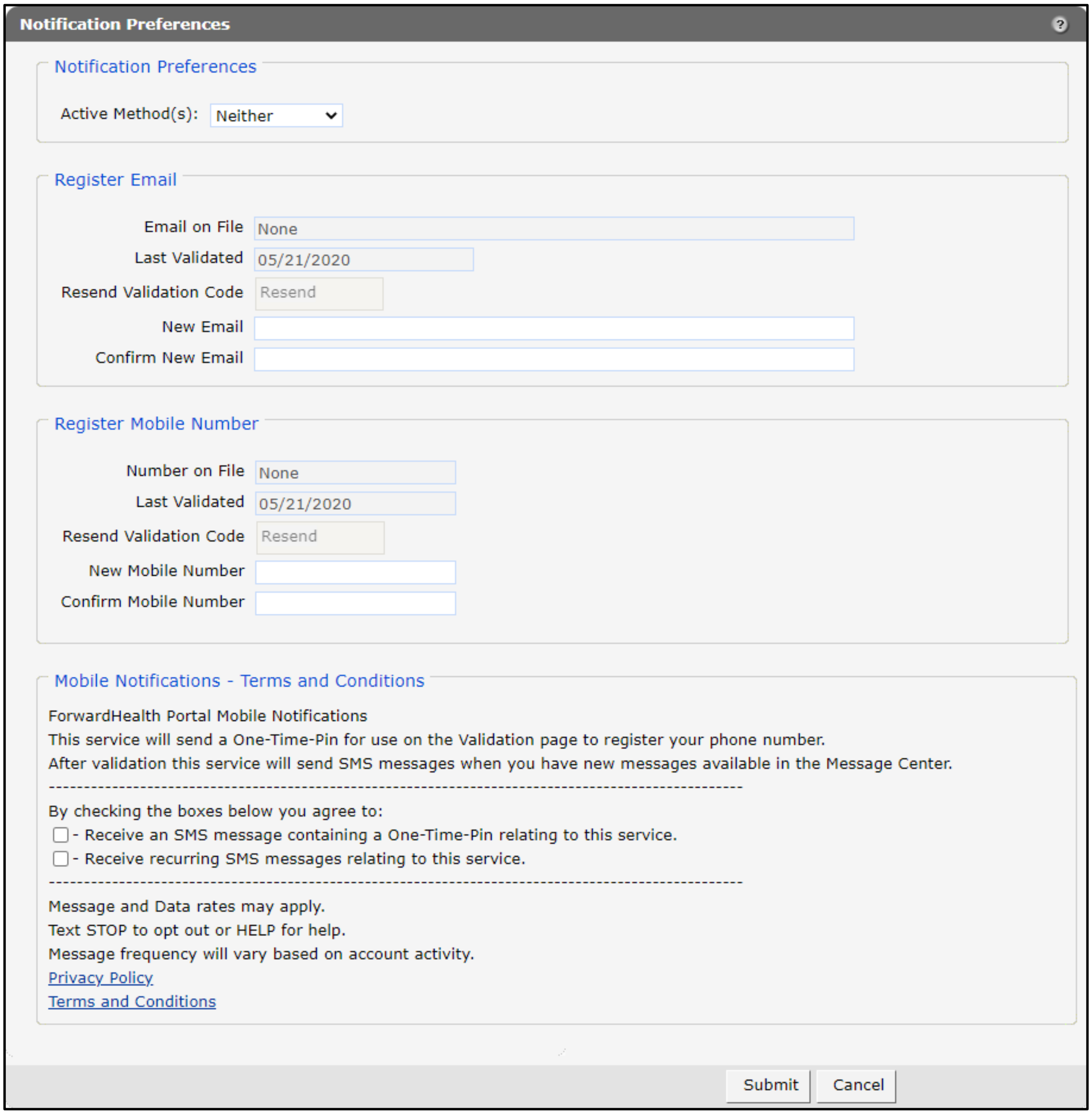


Figure 114 Notification Preferences Panel

2. Select the type of method in the *Active Method(s)* field using the drop-down menu.

3. If the user is registering to receive notifications via email, enter the user's email address in the *New Email* and *Confirm New Email* fields in the "Register Email" section.

4. If the user is registering to receive notifications via mobile phone, enter the user's mobile phone number in the *New Mobile Number* and *Confirm Mobile Number* fields in the "Register Mobile Number" section.

5. Check the appropriate agreement boxes to receive notifications via mobile phone.

6. Click **Submit**. A Notification Method Validation panel will be displayed, and a validation code will be sent to the email and/or mobile number that has been registered.

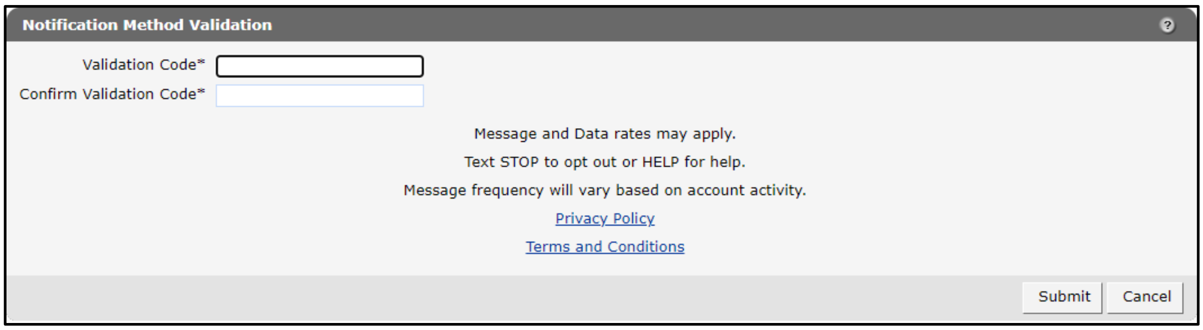


Figure 115 Notification Method Validation Panel

Note: The user can also access the Notification Method Validation panel by clicking **Validation Code** under Related Links.

7. Enter the validation code and click **Submit**. A confirmation message will be generated.

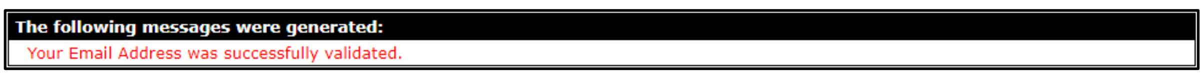


Figure 116 Confirmation Message

13 Trading Files

Providers are able to download provider-specific files, such as rate information, using the Trade Files function. Documents available for download using this function are those that have been uploaded by ForwardHealth for the individual provider(s).

1. On the Trade Files homepage, click **File Download**.

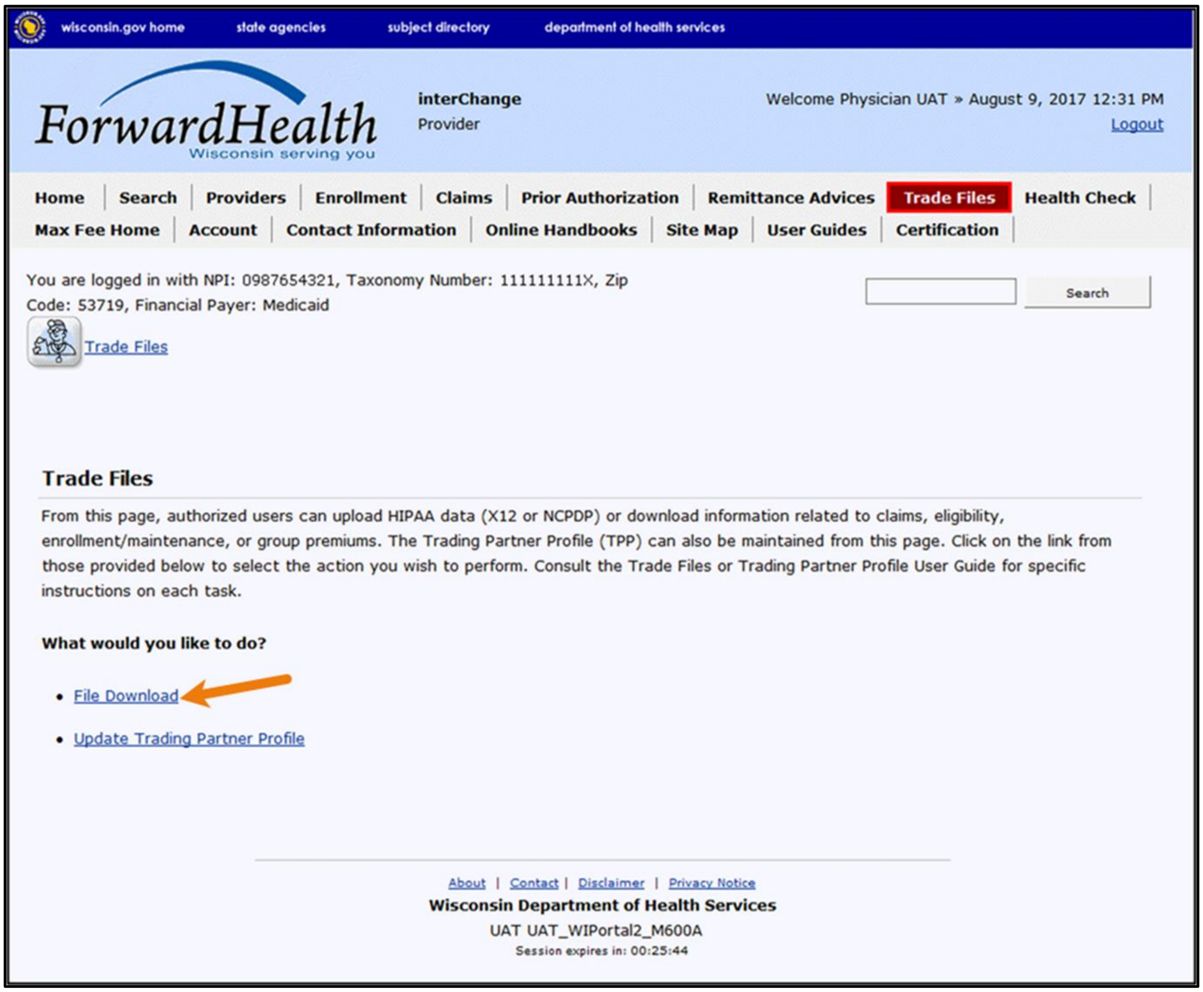


Figure 117 Trade Files Homepage

2. Select the applicable file type from the Transaction Type drop-down menu.

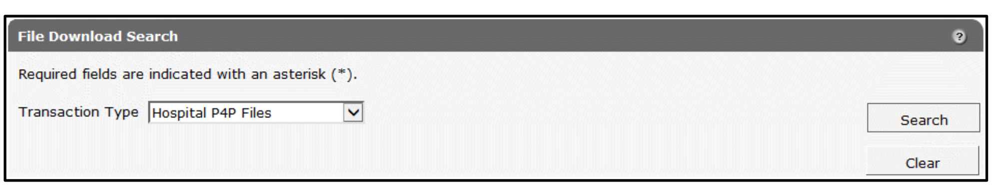
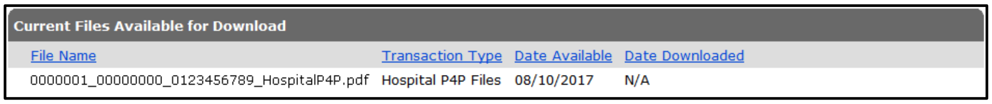


Figure 118 File Download Search Panel

3. Click **Search**.

4. Click the applicable file from the list under Current Files Available for Download.



Current Files Available for Download

File Name	Transaction Type	Date Available	Date Downloaded
0000001_00000000_0123456789_HospitalP4P.pdf	Hospital P4P Files	08/10/2017	N/A

Figure 119 Current Files Available for Download Panel

A download dialog box will be displayed.

Figure 120 Download Dialog Box

5. Click **Open**. The file will open and may be saved to the user's computer or network.

13.1 Avoiding Download Errors

If errors occur when downloading documents, try the following:

- Make certain to allow pop-ups on the Portal. In Internet Explorer:
  a. Go to Tools > Pop-up Blocker > Pop-up Blocker Settings.
  b. Add https://www.forwardhealth.wi.gov/ to the *Address of website to allow*.
- Add the Portal website to the list of Trusted Sites. For Internet Explorer:
  a. Go to Internet Options.
  b. Click the Security tab.
  c. Select Trusted sites.
  d. Click Sites.
  e. Add https://www.forwardhealth.wi.gov/ to the list.
- Set the **Trusted Sites security level** to the Medium-low default setting. For Internet Explorer:
  a. Go to Internet Options > Security.
  b. Click Trusted sites.
  c. Click Default level.
  d. Set the Security level slider to Medium-low.

14 Access interChange Functionality

The interChange (iC) Functionality section of the Provider area of the Portal allows authorized users to access member information.

1. To use interChange functionality on the Portal, click **iC Functionality** on the main menu at the top of the page. The iC Functionality page will be displayed.

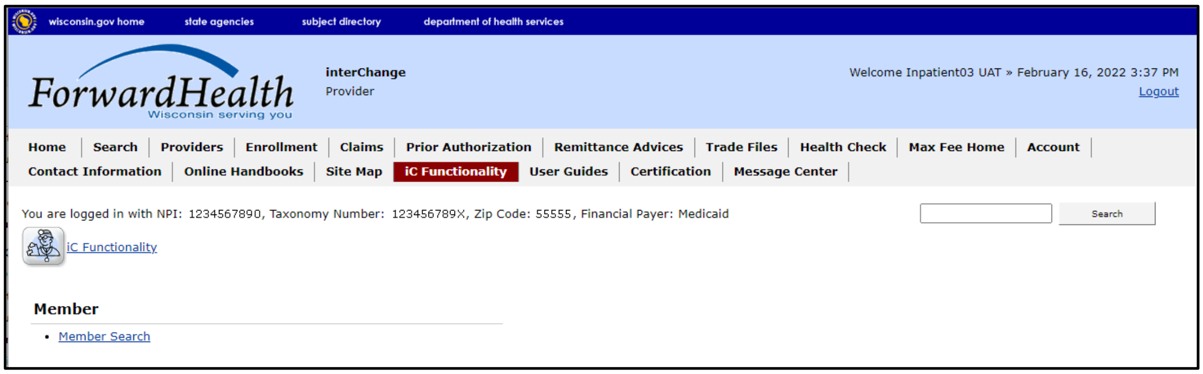


Figure 121 iC Functionality Page

15 Member

15.1 Member Search

1. On the iC Functionality page, click **Member Search**. The Member Search panel will be displayed.

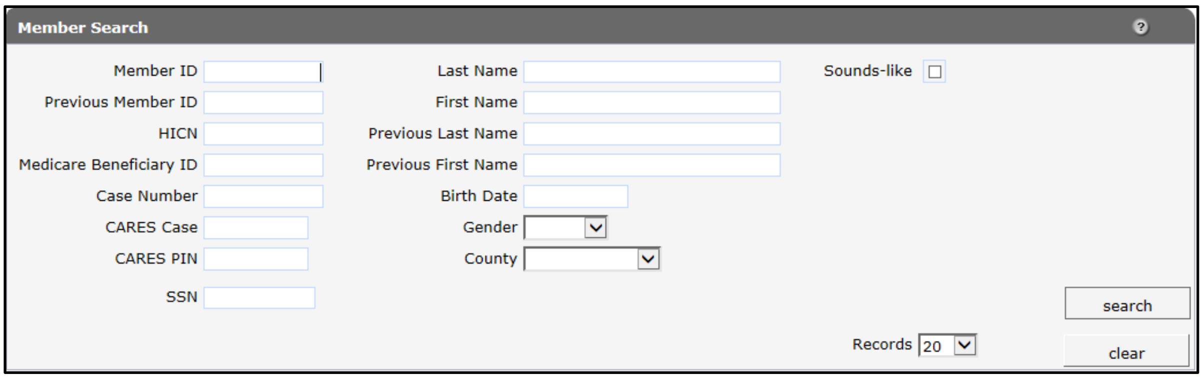


Figure 122 Member Search Panel

This user guide explains how to complete a member search using a member's name. Users can search for a member using any of the fields on the Member Search panel but should enter as much information as possible to narrow the results.

If a search returns too many results, a message will indicate that additional criteria must be entered. If a search does not return any results, a "No rows found" message will be displayed in the Search Results panel. Users should ensure that the entered information is accurate and correct any inaccurate information.

Note: If no results are found when searching using a member ID, enter the member's ID in the Previous Member ID field in case the member's ID has changed. If the member is found, the member's information will be displayed with his or her new ID.

The Search Results panel will display 20 results per page by default. To change the number of results that display, select another number from the Records drop-down menu.

To clear information from all the fields on the Member Search panel, click **clear**.

2. Enter the member's last name in the Last Name field.

   Check the **Sounds-like** box to perform a phonetic search on the member's last name. If the box is unchecked, an exact letter search will be performed.

3. Enter the member's first name in the First Name field.

4. Click **search**. If only one member record is found, the Member Information page will be displayed. If multiple member records matching the entered search criteria are found, the records will be displayed in the Search Results panel.

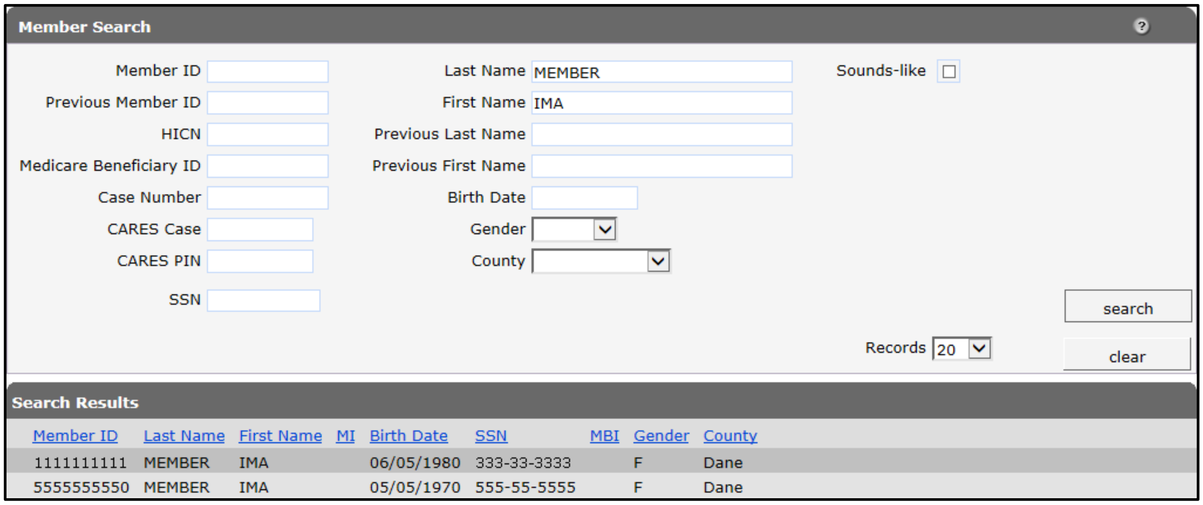


Figure 123 Search Results Panel

The member information will be displayed by column (for example, Member ID, Last Name, First Name). To sort the results, click a column heading. Clicking a column heading once will sort the results in ascending order by that column. Clicking a column heading twice will sort the results in descending order.

5. Click the applicable member record. The Member Information page will be displayed.

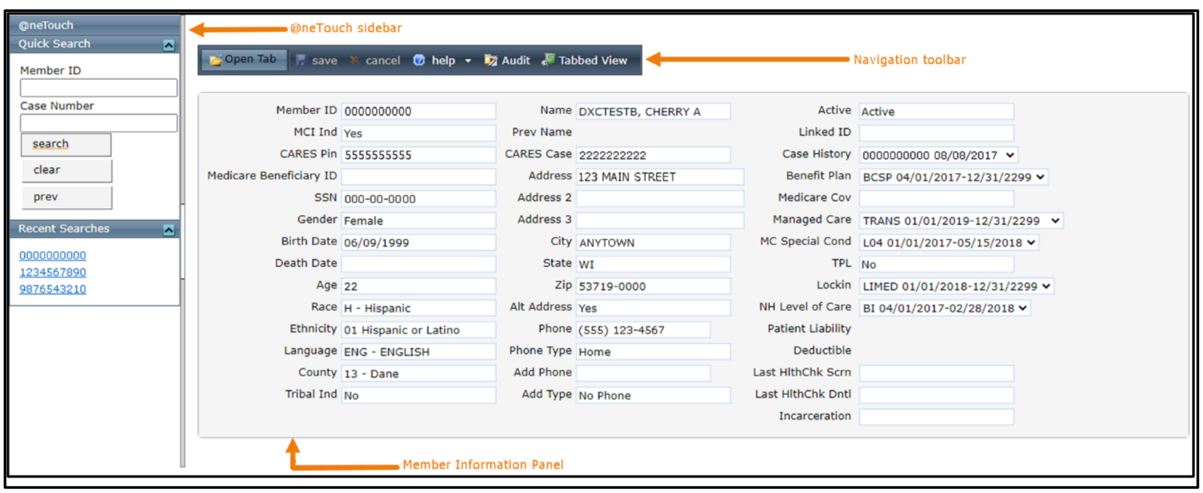


Figure 124 Member Information Page

The Member Information page consists of the following:

- @neTouch sidebar. The @neTouch sidebar contains a “Quick Search” section and a “Recent Searches” section.
    - The “Quick Search” section allows users to search for a new member record by entering either a member ID in the Member ID field or a Client Assistance for

Reemployment and Economic Support (CARES) case number in the Case Number field and clicking **search**. Users can click **clear** to delete information from the Member ID or Case Number fields or **prev** to return to the Member Search panel.

- The "Recent Searches" section displays the IDs of the last five members for whom users searched. Users can click an ID to populate that member's information in the Member Information panel. Both search sections can be minimized by clicking the arrow on the right.

- Navigation toolbar. The navigation toolbar contains the Open Tab menu, the Help menu, and the Stacked/Tabbed View function. The other functions are unavailable.
  - The *Open Tab* menu provides access to panels that contain more detailed member information.
  - The *Help* menu provides access to information regarding the Member Information panel (Page Specific Help) or the panels available under the Open Tab menu (Tab Specific Help). A panel from the Open Tab menu must be selected for the Tab Specific Help option to be available.
  - The *Stacked/Tabbed View* function allows users to choose whether to display the panels available under the Open Tab menu in a stacked or tabbed view. In the stacked view, all panels that have been selected from the Open Tab menu will display together beneath the Member Information panel. In the tabbed view, the panels will display on different tabs located across the top of the panel, and users can switch between the panels by clicking the tabs. The shortcut for switching between the stacked and tabbed views is Alt+o. The screen captures in this user guide display the tabbed view option.
- Member Information panel.

15.1.1 Member Information Panel

The Member Information panel displays basic data about a member.

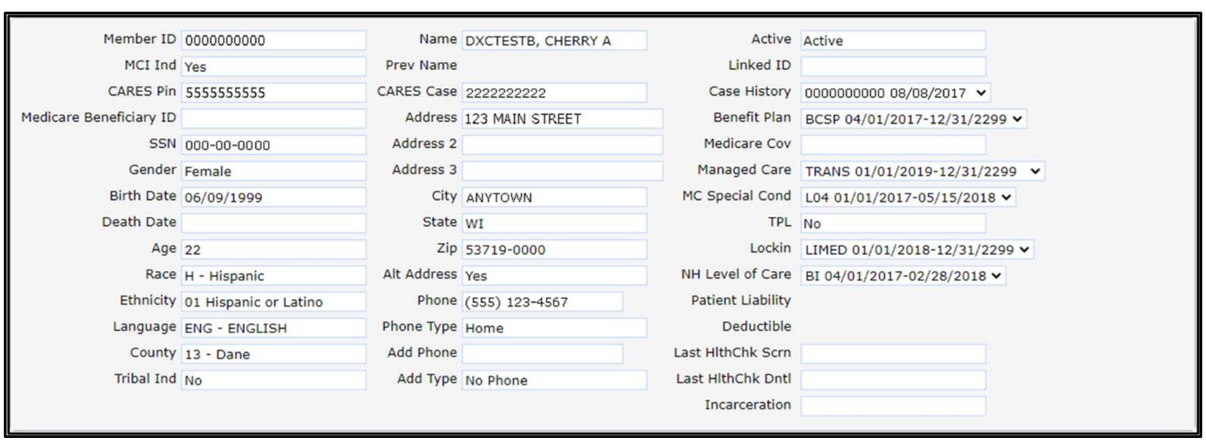


Figure 125 Member Information Panel

The left column displays some of the following information:

- The *MCI Ind* field indicates whether or not a Master Client Index (MCI) indicator was assigned. The field will indicate *Yes* if the member's ID was assigned from the MCI database and *No* if the member's ID is temporary.
- The *CARES Pin* field displays the member's CARES personal identification number.
- The member's demographic data.

The middle column displays some of the following information:

- The member's name and previous name, if applicable.
- The member's CARES case number.
- The member's contact information.

The right column displays applicable member enrollment information such as the following:

- The *Active* field indicates *Active* if the ID in the Member ID field is current or *Inactive* if the ID is no longer used. If *Inactive* is displayed and the member has a more current ID, the most current ID would be displayed in the Linked ID field.

  Note: Throughout this user guide, an *Active* status indicates that the displayed information is current. An *Inactive* or *History* status indicates that the displayed information is no longer used or is invalid. Inactive or historical information is maintained for informational or auditing purposes only.

- The *Linked ID* field displays information if the member has another ID that is linked to the member's present ID.
- The *Case History* menu displays the case ID with which the member is associated and the date(s) that the member's case ID was applied to interChange.
- The *Benefit Plan* menu displays the benefit plan(s) in which a member is or was enrolled. The field includes a benefit plan code and the effective dates of each plan.

  Note: An end date of 12/31/2299 signifies an open end date.

- The *Medicare Cov* field displays the member's current Medicare coverage. The field may show one or more of the following:

  a. *A* indicates Medicare Part A.

  b. *B* indicates Medicare Part B.

  c. *D* indicates Medicare Part D.

  The field will be blank if the member does not have current coverage.

- The *Managed Care* field indicates if the member is enrolled in a BadgerCare Plus HMO, Medicare Supplemental Security Income (SSI) HMO, Family Care, Program for All Inclusive

Care for the Elderly, Family Care Partnership, or a children's health managed care plan (for example, Children Come First, Wraparound Milwaukee). The field also displays the effective and end dates of the member's enrollment.

- The *MC Special Cond* field displays the member's Managed Care Special Condition level of care (LOC) if they are enrolled in a long-term care managed care program and/or the member's exemption information, if applicable. The field also displays the effective and end dates related to the member's LOC or exemption.
- The *TPL* field displays a *Yes* or a *No* to indicate whether or not the member has current third-party (private) insurance coverage.
- The *Lockin* field indicates if the member is restricted to specific providers or if the member is enrolled in a hospice program. If a lock in is in effect, the effective and end dates will also be displayed.
- The *NH Level of Care* field displays nursing home LOC codes not related to managed care. The field also displays the effective and end dates of the member's LOC authorization.
- The *Patient Liability* field displays the monthly institutional liability or waiver cost share amounts the member must contribute to their cost of care. The field also displays the effective and end dates of the cost share.
- The *Deductible* field indicates the member's current SeniorCare deductible and the effective and end dates for which the member's SeniorCare deductible was applied. This field does not apply to private insurance.
- The *Last HlthChk Scrn* field displays the date of the member's last HealthCheck screening.
- The *Last HlthChk Dntl* field displays the date of the member's last dental screening that was provided as a HealthCheck service.
- The *Incarceration* field indicates the incarceration effective date and end date for members with active incarceration information.

15.1.2 Open Tab Menu

Hover over Open Tab on the navigation toolbar to display the Open Tab menu. The Open Tab menu displays seven different menu options; however, only the Member menu option is available.

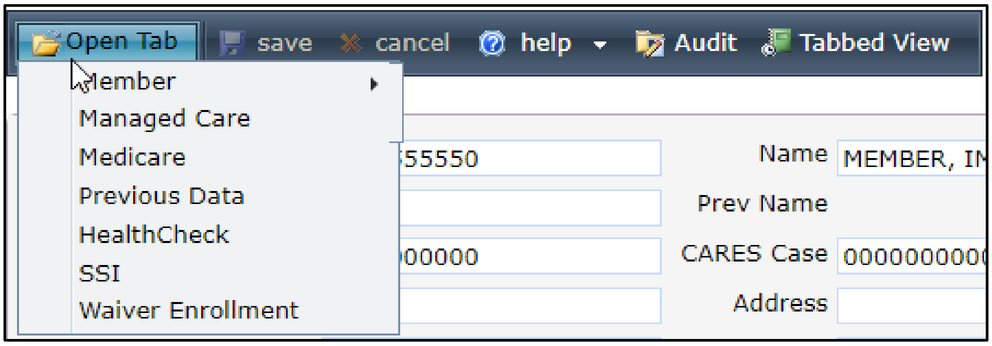


Figure 126 Open Tab Menu

Member Menu

Hover over Member on the Open Tab menu to display menu options for panels containing a member's base information and review status.

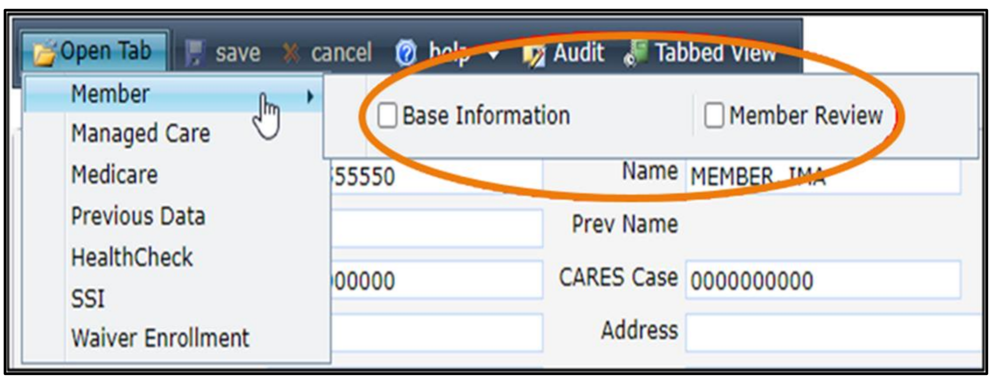


Figure 127 Member Menu

Panels listed under menus operate under the following principles:

- Clicking a panel name will open the selected panel.
- Checking the box next to the panel name causes the panel to automatically display each time that menu is accessed, even in subsequent Portal sessions.
- Panel names that are highlighted indicate the panel is currently open.
- Panel names that are italicized indicate the panel is inaccessible to the user.

Base Information Panel

The Base Information panel displays basic information about a member.

1. Select **Base Information** from the Member Menu. The Base Information panel will be displayed.

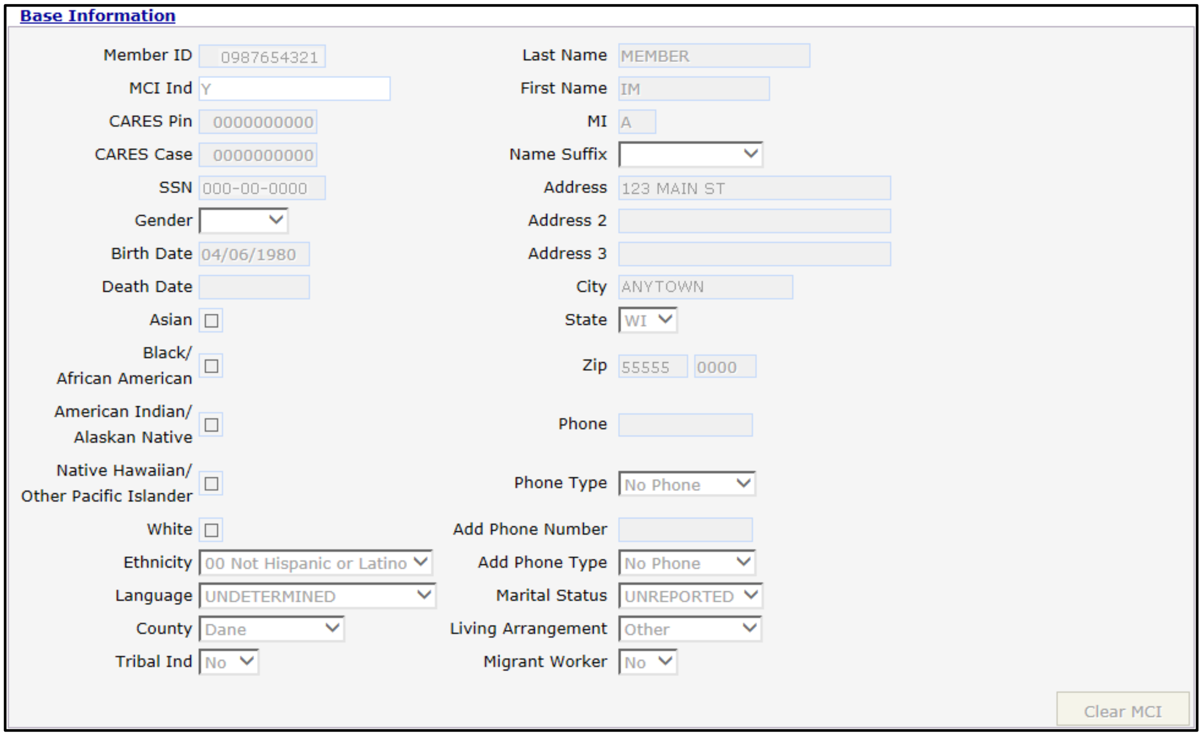


Figure 128 Base Information Panel

Member Review Panel

The Member Review panel displays if a member is on review and describes why.

1. Click **Member Review** from the Member menu. The Member Review panel will be displayed.
2. Click the applicable row to populate information in the fields on the panel.

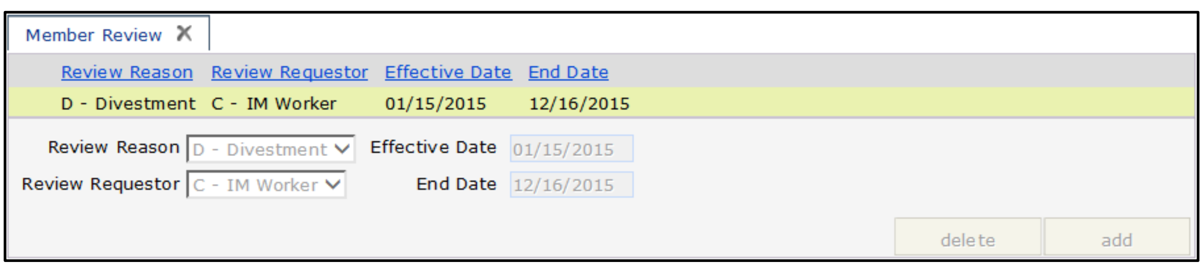


Figure 129 Member Review Panel

The Member Review panel may include the following information:

- The *Review Reason* field indicates the reason the member was put on review (for example, Divestment).

  Note: Divestment information is sent to interChange through the CARES interface. The ForwardHealth Call Center will review the penalty period start date before the information is added to interChange and will consider adverse action and notice requirements.

- The *Review Requestor* indicates the person who determined that the member should be put on review (for example, IM Worker).
- The *Effective Date* field displays the first date of service (DOS) the member review is effective.
- The *End Date* field displays the last DOS the member review is effective.

16 Appendix: Portal Help Desk Support

Users may contact the Portal Helpdesk with questions about configuring supported web browsers or technical questions on Portal functions, including Portal accounts, registrations, passwords, and submissions through the Portal.

- Phone: 866-908-1363
- Email: vedswiedi@wisconsin.gov