User Guide

Electronic Visit Verification Portal Functionality

August 11, 2025

WISCONSIN DEPARTMENT of HEALTH SERVICES

Table of Contents

1 Introduction ... 3

2 Provider Enrollment ... 4

3 Request Portal Access ... 11

4 Set Up an Account ... 17
  4.1 Logging in for First Time ... 17
  4.2 Reset Password ... 23
  4.3 Unlocking An Account ... 37
  4.4 Account Types ... 47

5 Clerk Maintenance ... 49
  5.1 Add a Clerk ... 51
  5.2 Search for a Clerk ... 53
  5.3 Add a Role to a Clerk ... 54
  5.4 Remove a Role From a Clerk ... 57
  5.5 Assign a Clerk Administrator ... 59
  5.6 Reset a Clerk's Password ... 60
  5.7 Delete a Clerk Account ... 61
  5.8 Clerk Account Log in for First Time ... 61

6 Clerk Last Logon ... 72
  6.1 Search and Remove a Clerk Account ... 72

7 Demographic Maintenance Tool ... 74

8 Worker Association ... 78
  8.1 Add Worker ... 79
    8.1.1 No Matches Found ... 80
    8.1.2 Match Found ... 82
  8.2 Upload Worker File ... 84

9 Manage Workers ... 88

10 List of Workers Within Your Agency 93

1 Introduction

Electronic visit verification (EVV) is a system that uses technology to make sure that members and participants receive the services they need. Workers check in at the beginning and check out at the end of each visit, using a smart phone or tablet, small digital device, or landline phone.

Setting up a secure ForwardHealth Provider Portal account will start the training process with the Wisconsin Department of Health Services (DHS) EVV system. A Portal account also allows the provider to conduct business with DHS, including maintaining worker information and making updates to business information. ForwardHealth brings together many DHS health care programs with the goal to create efficiencies for providers and to improve health outcomes for enrolled members.

2 Provider Enrollment

In order for EVV information to be correctly associated to claims and encounters, DHS requires all providers and workers to have a Medicaid provider ID number regardless of the EVV-system used. To generate this ID, providers will need to follow the steps below.

1. Access the ForwardHealth Portal (the Portal) at forwardhealth.wi.gov/.

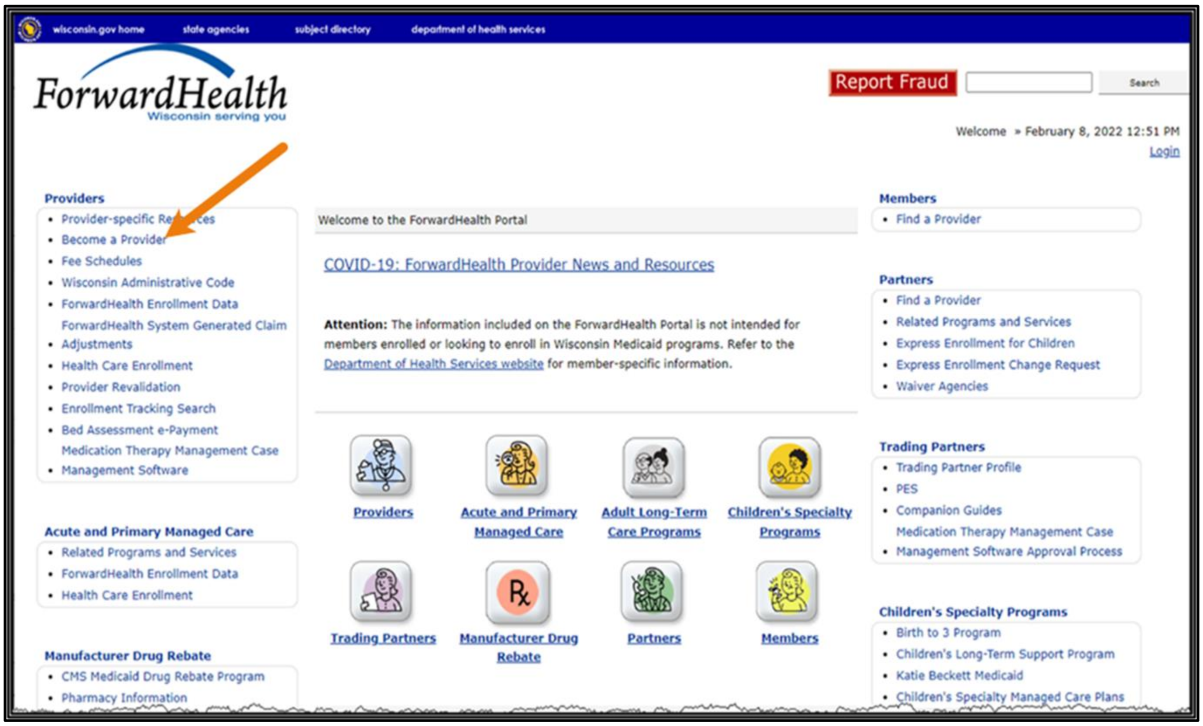


Figure 1 Portal Homepage

2. Click **Become a Provider**. The Provider Enrollment Information page will be displayed.

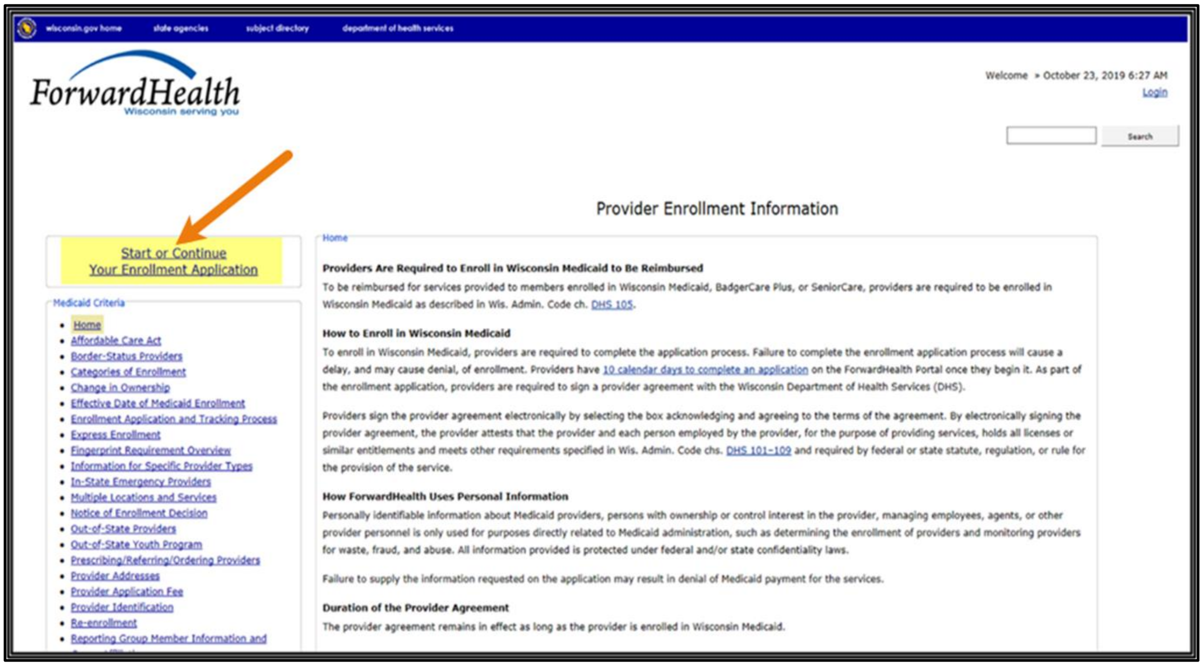


Figure 2 Provider Enrollment Information Page

3. Click **Start or Continue Your Enrollment Application**. The Enrollment Application page will be displayed.

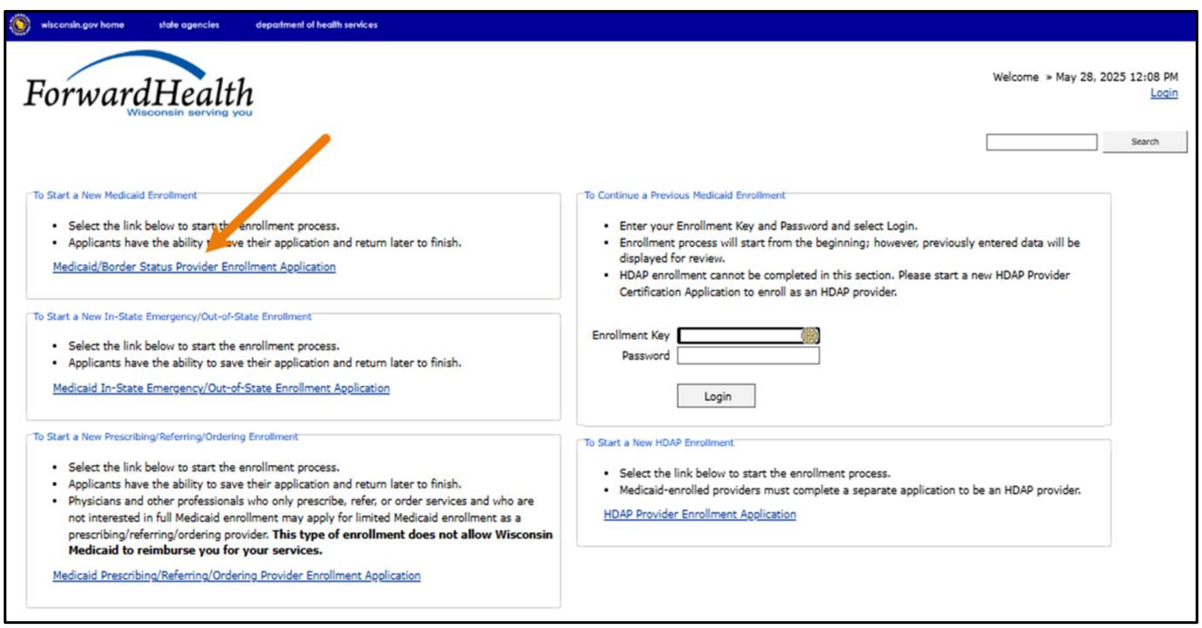


Figure 3 Enrollment Application Page

4. Click **Medicaid/Border Status Provider Enrollment Application**.

The Instructions panel will be displayed.

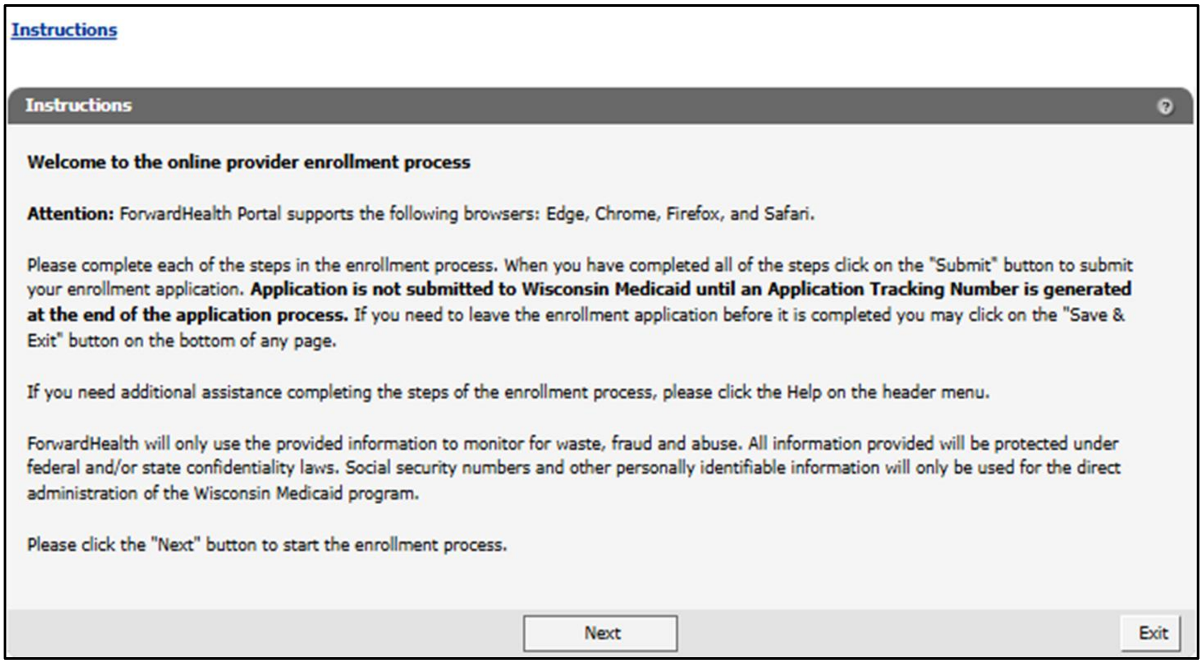


Figure 4 Instructions Panel

5. Read the instructions. Click **Next** to continue. The Type of Applicant panel will be displayed.

   Note: All required fields are indicated with an asterisk (*).

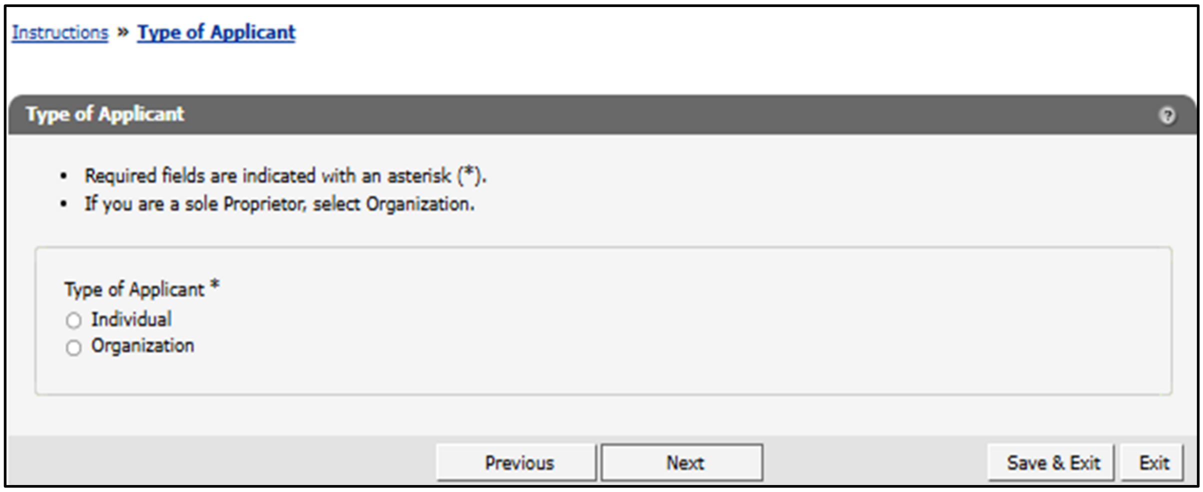


Figure 5 Type of Applicant Panel

6. Select **Organization** under **Type of Applicant***.
7. Click **Next**. The Type of Enrollment panel will be displayed.

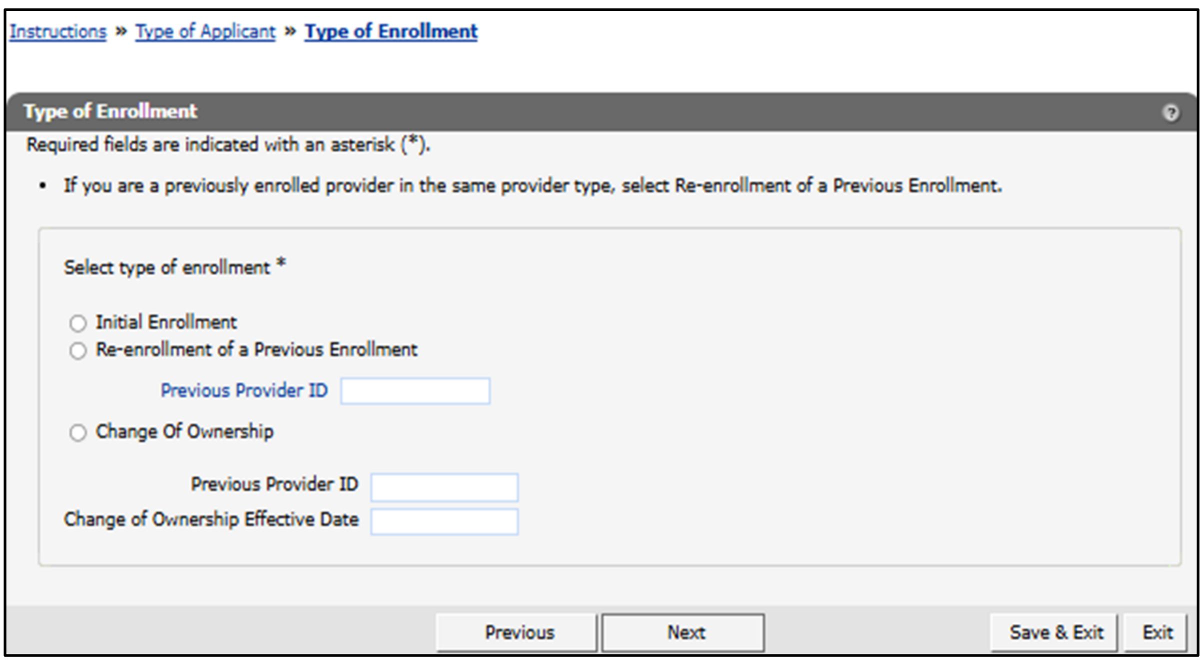


Figure 6 Type of Enrollment Panel

8. Select Initial Enrollment.
9. Click **Next**.

The Provider Type panel will be displayed.

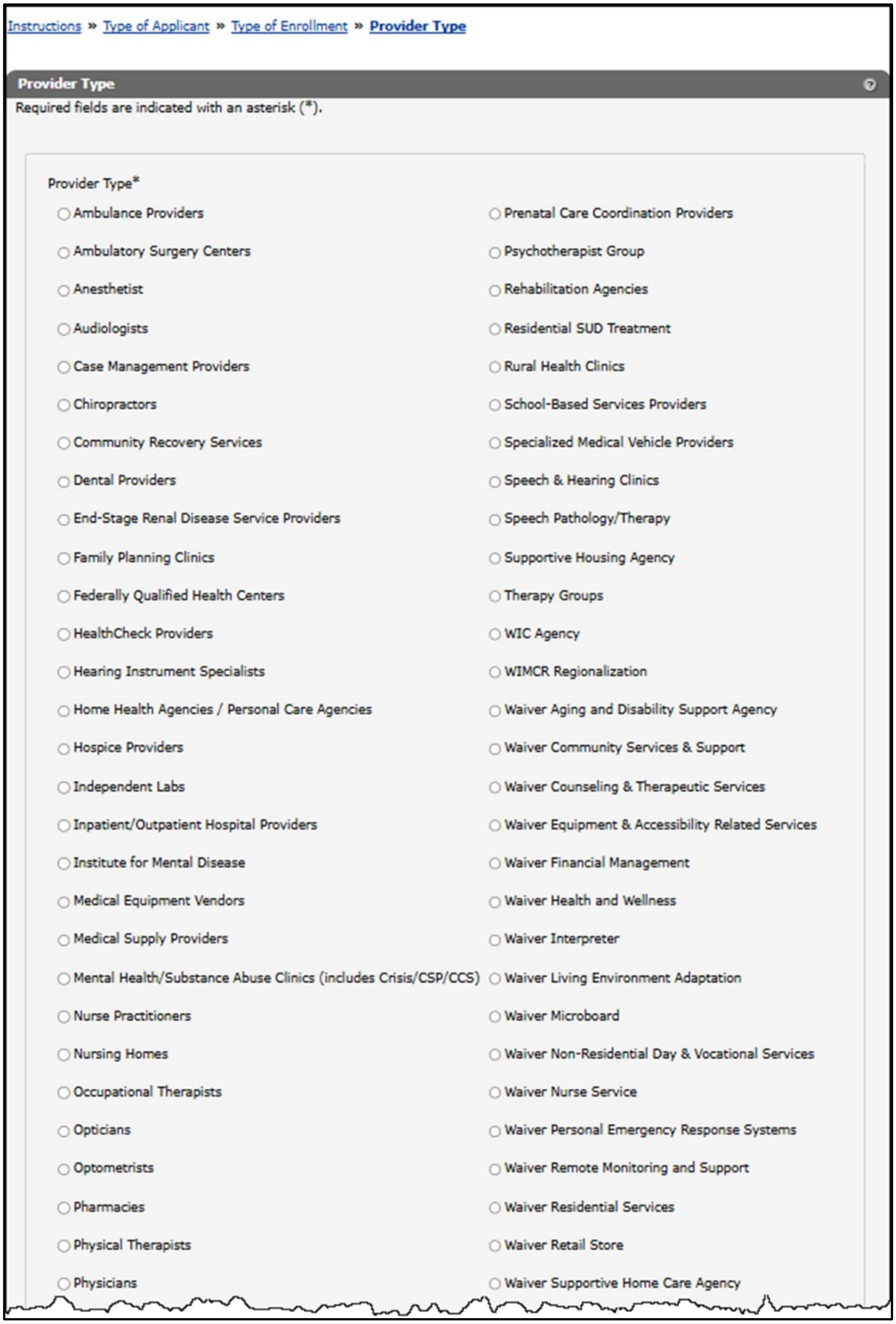


Figure 7 Provider Type Panel

10. Select **Waiver Supportive Home Care Agency**.

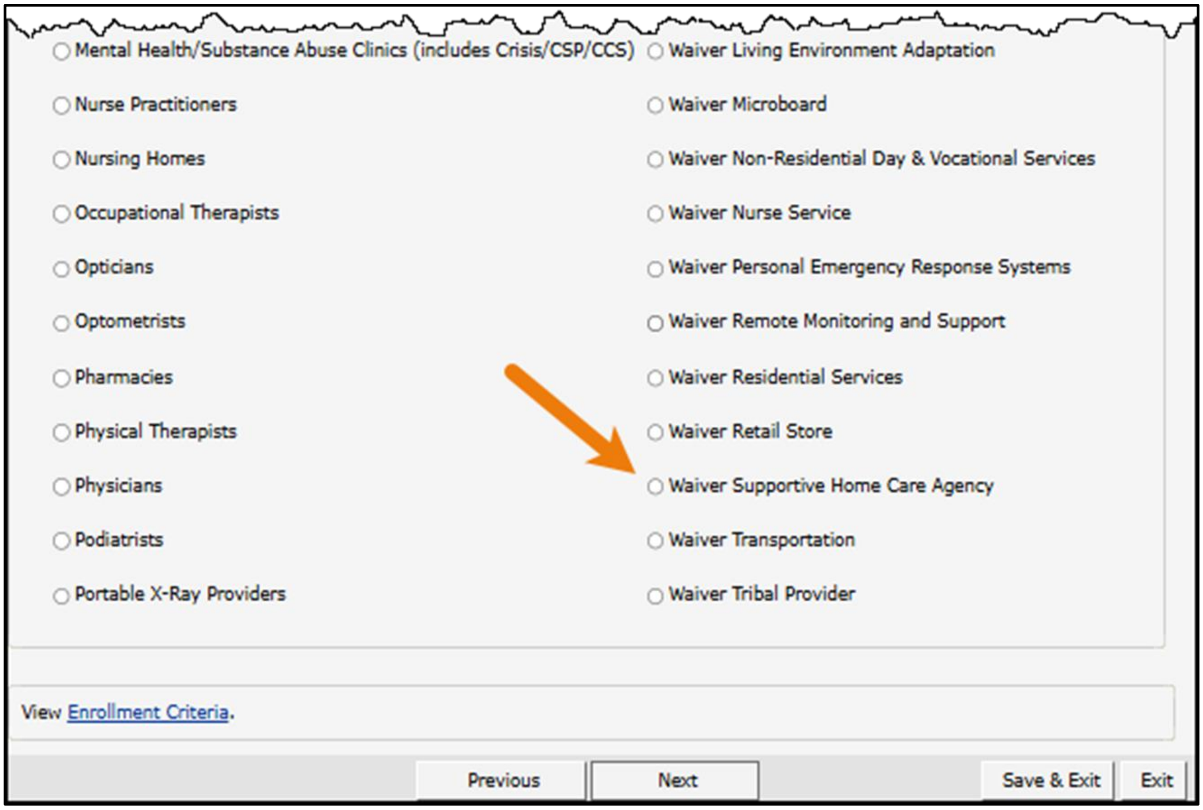


Figure 8 Provider Type Panel—Waiver Support Home Care Agency

11. Click **Next**. The LTC Waiver Provider Service Enrollment panel will be displayed.

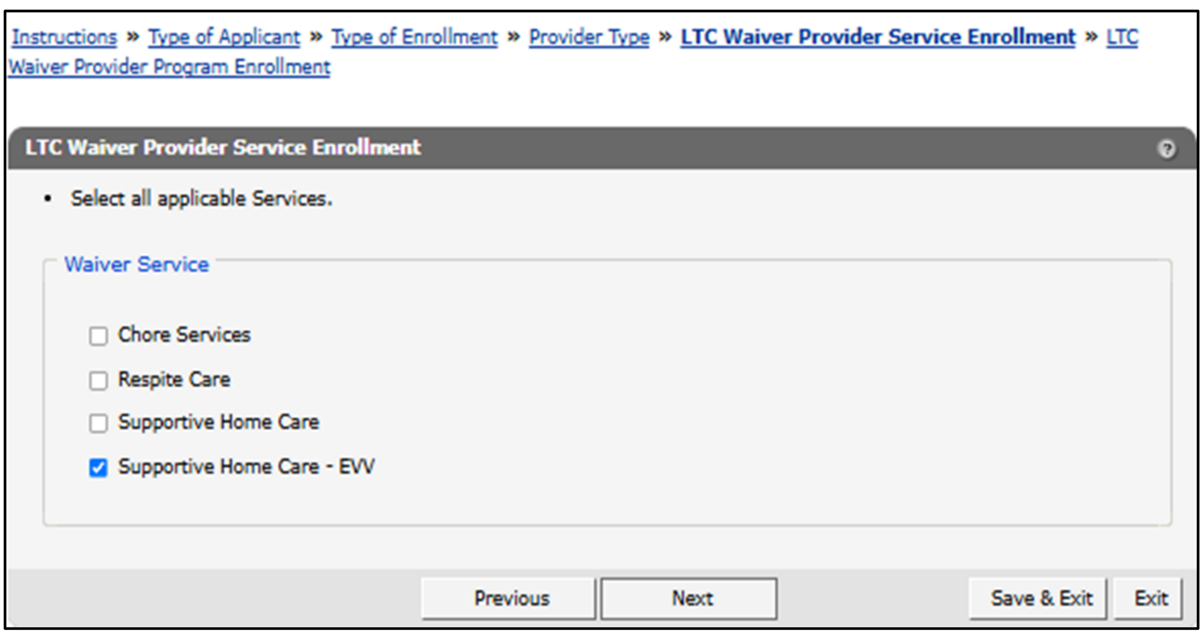


Figure 9 LTC Waiver Provider Service Enrollment Panel

12. Select Supportive Home Care – EVV and any other applicable services.

13. Click **Next**. The LTC Waiver Provider Program Enrollment panel will be displayed.

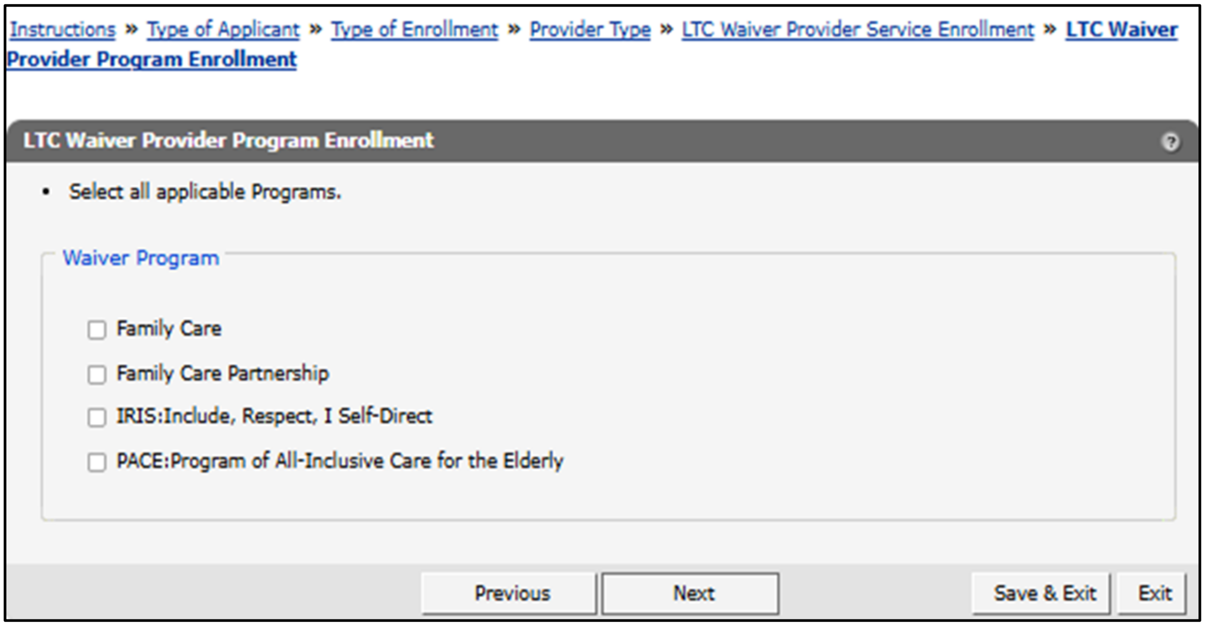


Figure 10 LTC Waiver Provider Program Enrollment Panel

14. Select all applicable waiver program(s).

15. Click **Next**.

16. Follow the on-screen prompts and complete the remaining provider enrollment application information. Note: The user can save and exit a provider enrollment application at any time by clicking **Save & Edit** at the bottom right of the screen.

17. Submit the completed provider enrollment application request. Note: ForwardHealth usually notifies the provider of their enrollment status within 10 business days after receiving the **complete** enrollment application, but no longer than 60 days.

18. Once the provider enrollment application request has been approved, the provider can request Portal access.

3 Request Portal Access

Providers will need a PIN to establish a Provider Portal account. Providers can establish as many provider Portal accounts as needed for their business.

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

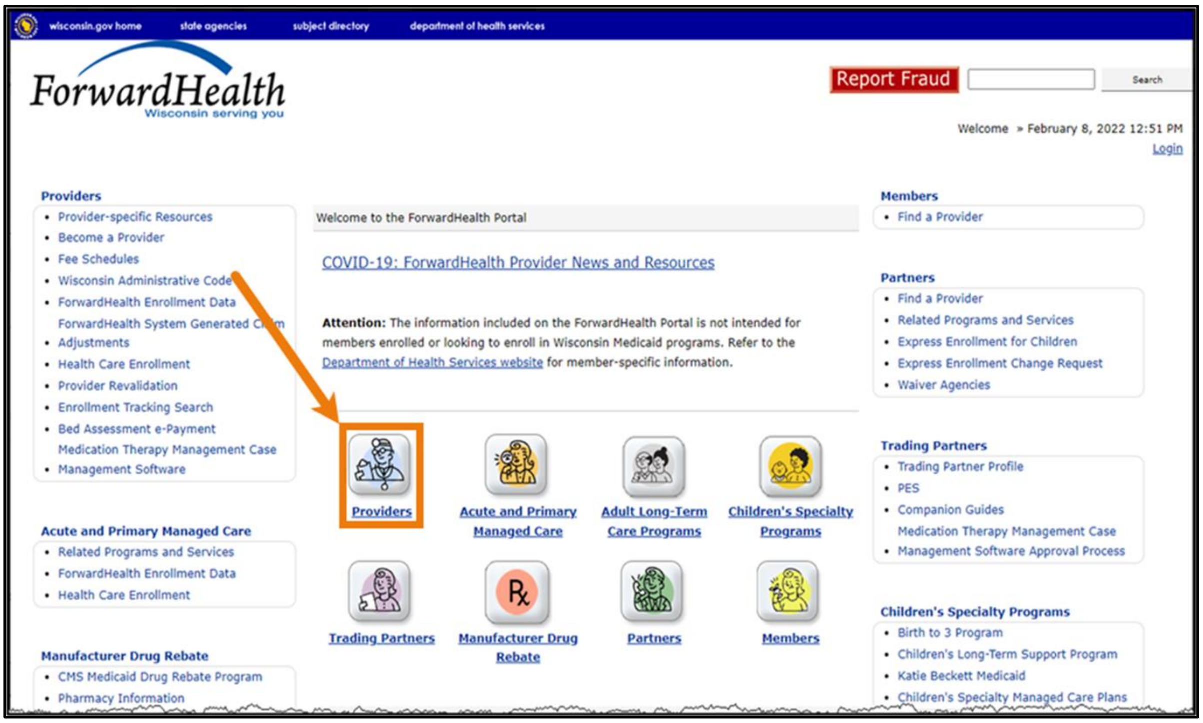


Figure 11 Portal Homepage

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

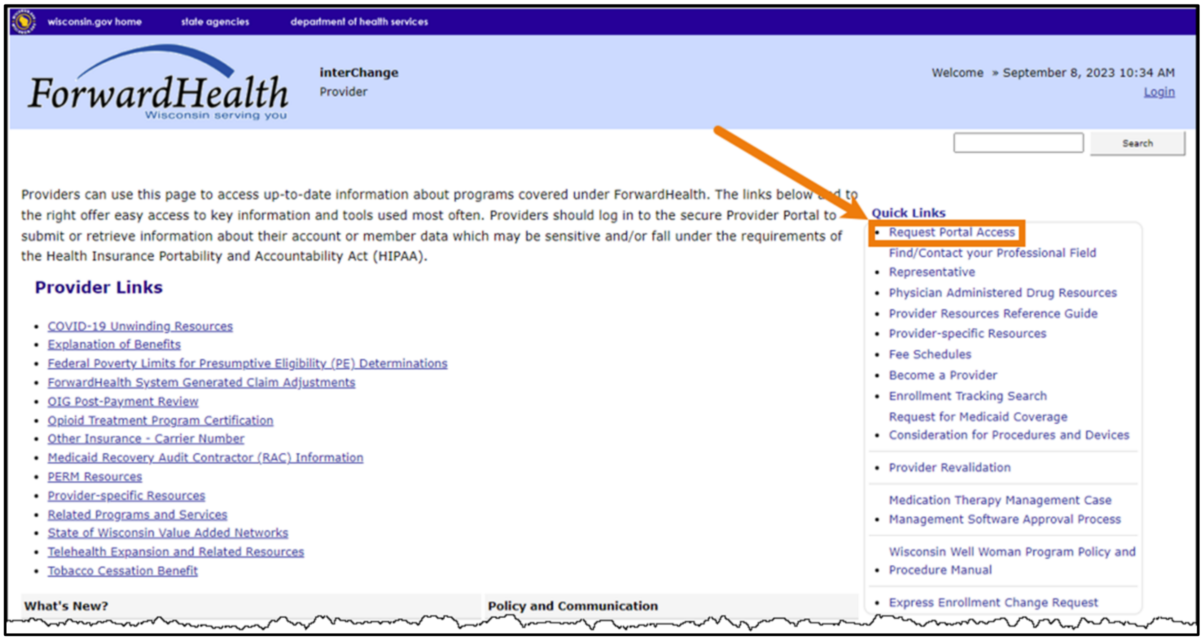


Figure 12 Public Provider Page

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

   The Request Portal Access page will be displayed.

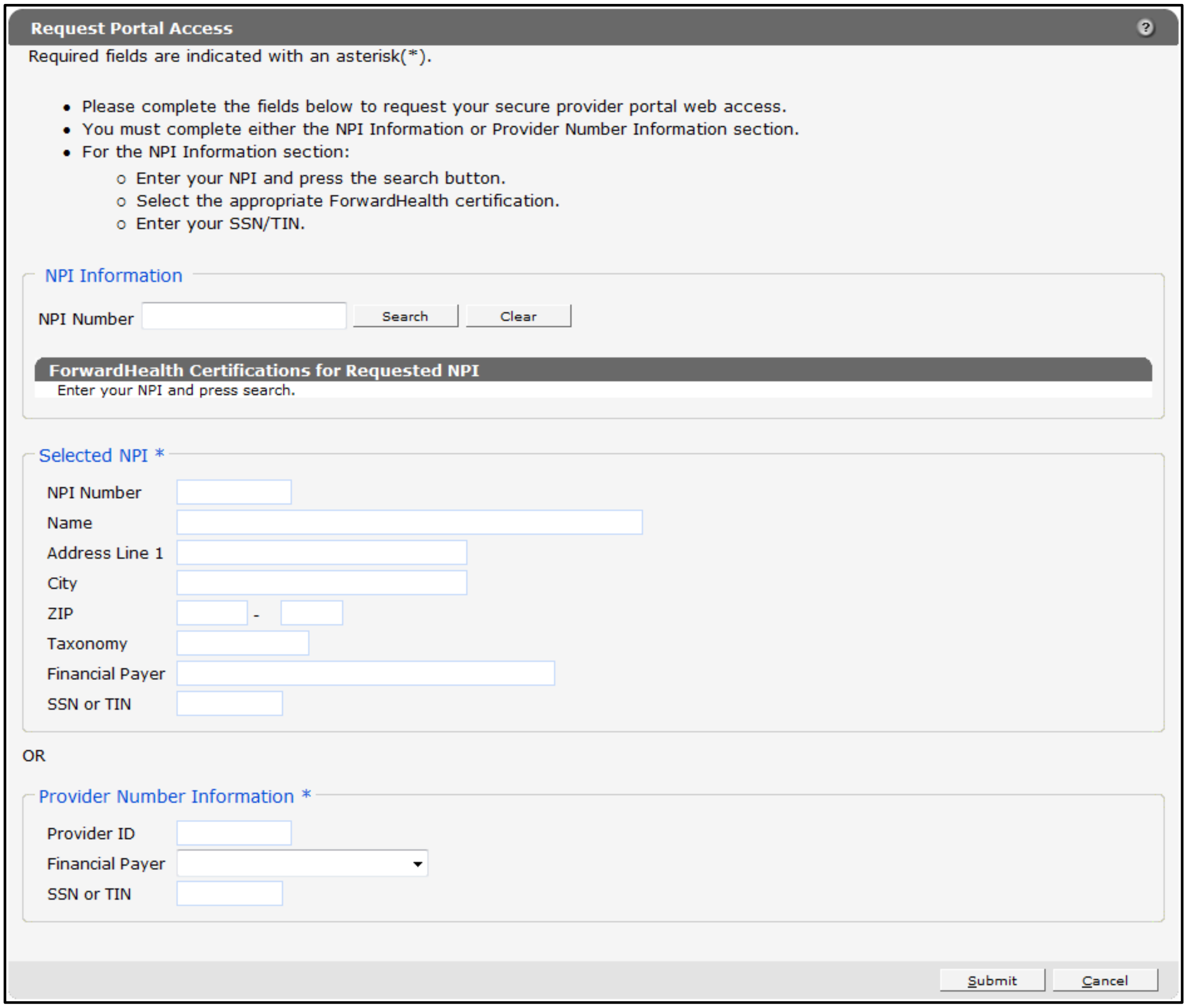


Figure 13 Request Portal Access Page

4. Complete **either** the "Selected NPI" or "Provider Number Information" sections. 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.

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

6. Enter the provider's Social Security Number (SSN) or Taxpayer Identification Number (TIN) in the SSN or TIN field.

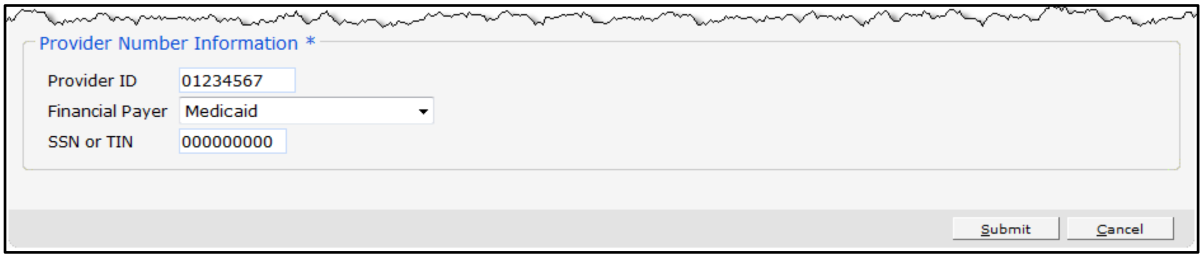


Figure 14 Provider Number Information Section

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

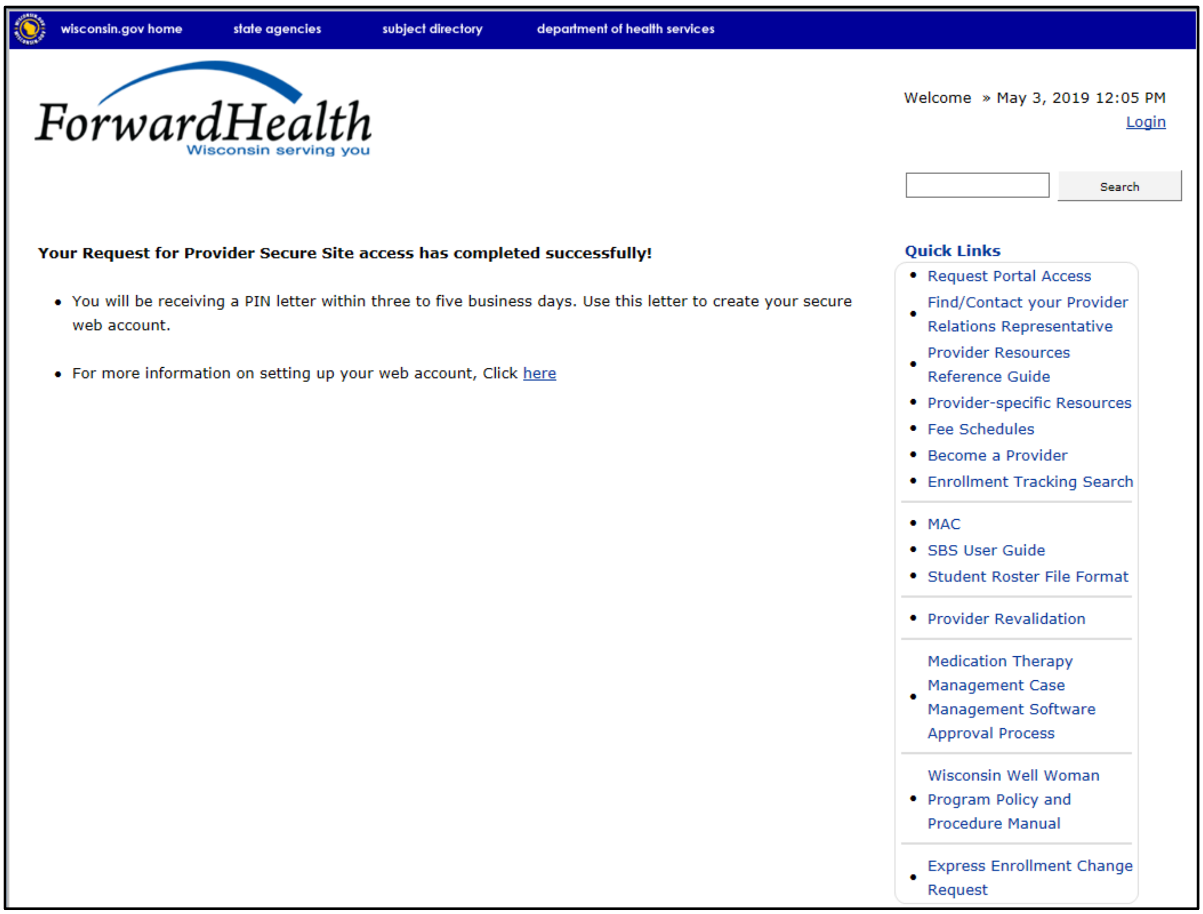


Figure 15 Confirmation Page

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.

The following messages were generated:
The PIN request has been rejected. A unique ForwardHealth certification could not be identified for the requested SSN/TIN.

Figure 16 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–Friday,8:30 a.m.–4:30 p.m.

After a provider has successfully requested Portal access, a letter containing a Personal Identification Number (PIN) will be mailed to the provider within three to five business days. 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 17 PIN Letter

4 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 username and password as well as to enter contact and security information.

4.1 Logging in for First Time

1. After the PIN letter is received, access the Portal at forwardhealth.wi.gov/.

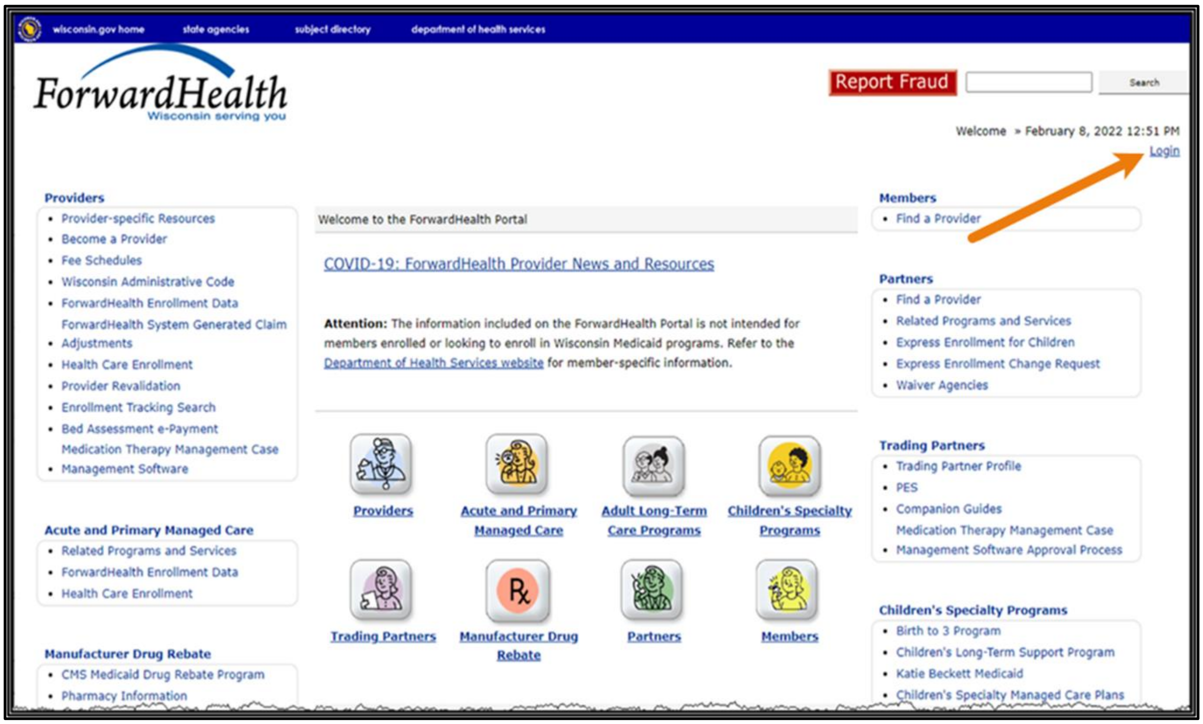


Figure 18 Portal Homepage

2. Click **Login**.

3. A Sign In box will be displayed.

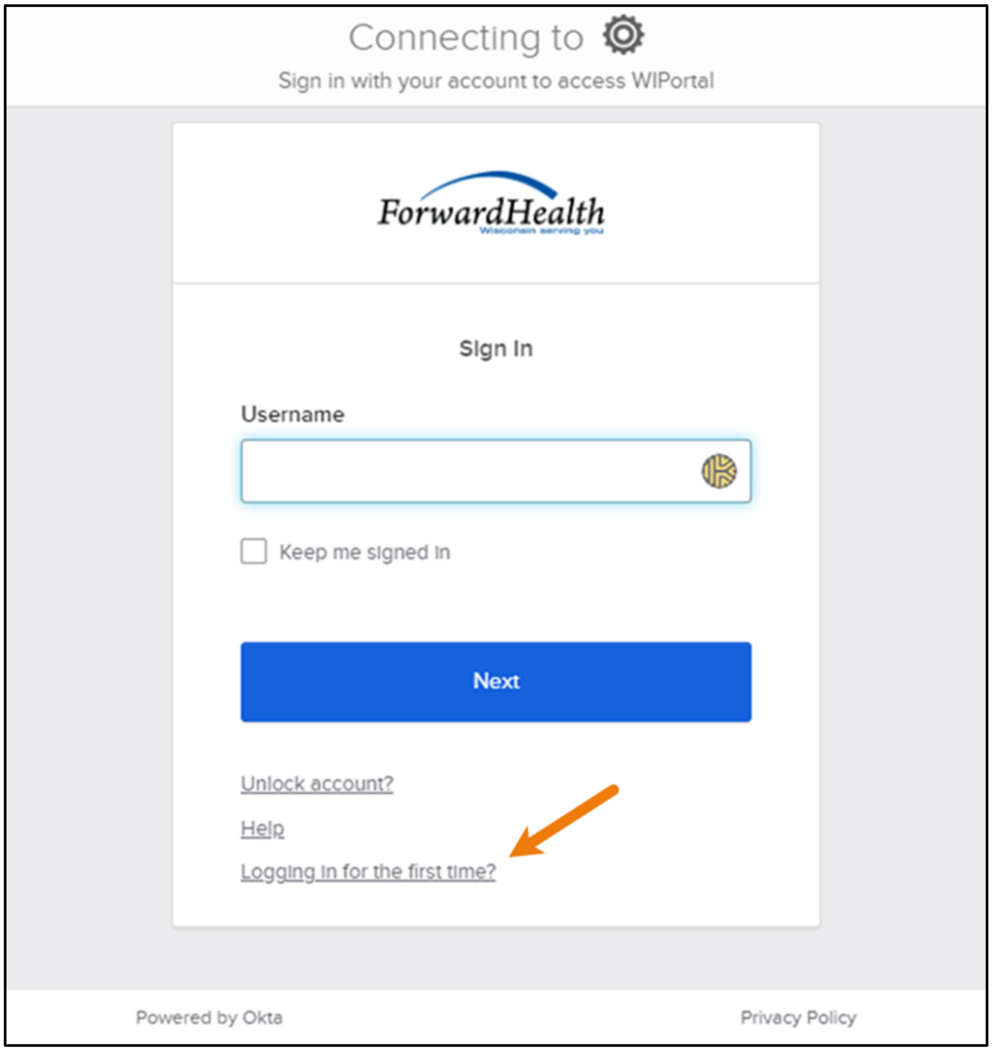


Figure 19 Sign-In Box

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

The Account Setup page will be displayed.

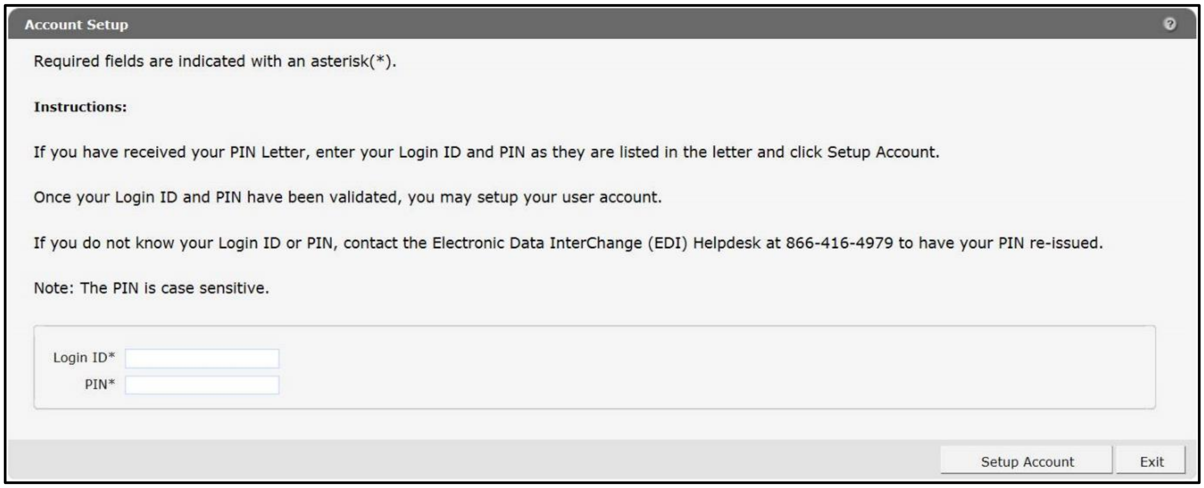


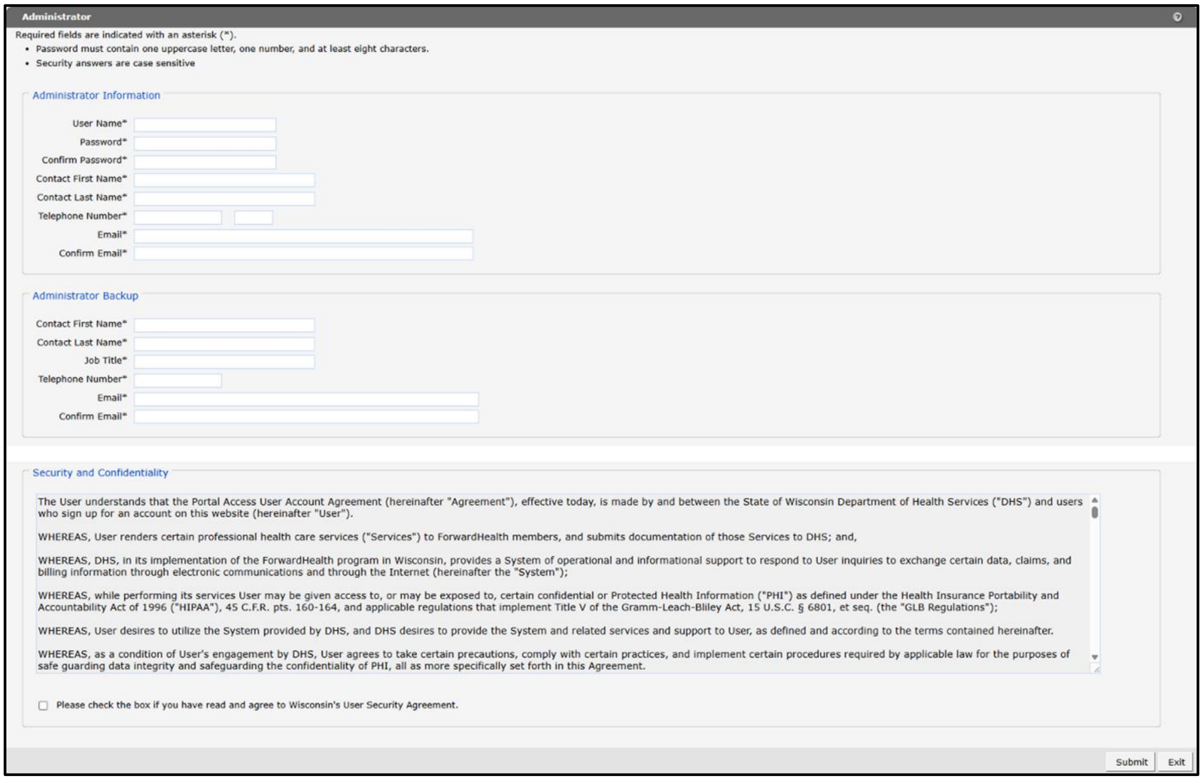
Figure 20 Account Setup Page

5. Enter the Login ID and PIN listed in the PIN letter.

   For security purposes, the PIN letter will contain only four digits of the Provider ID reported; however, users should **enter their entire** 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.

6. Click **Setup Account**. The Administrator setup page will be displayed.


Administrator

Required fields are indicated with an asterisk (*).

- Password must contain one uppercase letter, one number, and at least eight characters.
- Security answers are case sensitive

Administrator Information

User Name*
Password*
Confirm Password*
Contact First Name*
Contact Last Name*
Telephone Number*
Email*
Confirm Email*

Administrator Backup

Contact First Name*
Contact Last Name*
Job Title*
Telephone Number*
Email*
Confirm Email*

Security and Confidentiality

The User understands that the Portal Access User Account Agreement (hereinafter "Agreement"), effective today, is made by and between the State of Wisconsin Department of Health Services ("DHS") and users who sign up for an account on this website (hereinafter "User").

WHEREAS, User renders certain professional health care services ("Services") to ForwardHealth members, and submits documentation of those Services to DHS; and,

WHEREAS, DHS, in its implementation of the ForwardHealth program in Wisconsin, provides a System of operational and informational support to respond to User inquiries to exchange certain data, claims, and billing information through electronic communications and through the Internet (hereinafter the "System");

WHEREAS, while performing its services User may be given access to, or may be exposed to, certain confidential or Protected Health Information ("PHI") as defined under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 45 C.F.R. pts. 160-164, and applicable regulations that implement Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, et seq. (the "GLB Regulations");

WHEREAS, User desires to utilize the System provided by DHS, and DHS desires to provide the System and related services and support to User, as defined and according to the terms contained hereinafter.

WHEREAS, as a condition of User's engagement by DHS, User agrees to take certain precautions, comply with certain practices, and implement certain procedures required by applicable law for the purposes of safe guarding data integrity and safeguarding the confidentiality of PHI, all as more specifically set forth in this Agreement.

Please check the box if you have read and agree to Wisconsin's User Security Agreement.

Submit Exit

Figure 21 Account User Profile Page

7. Enter information in the fields for the Administrator Information and Administrator Backup sections. 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 automatically format.

   Note: The administrator backup email addresses cannot match those of the current administrator.

8. Read the Security and Confidentiality agreement.

9. Check the agreement checkbox.

10. Click **Submit**. If an error message is received, 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. This allows users to access the secure Portal as they are billing Medicaid.

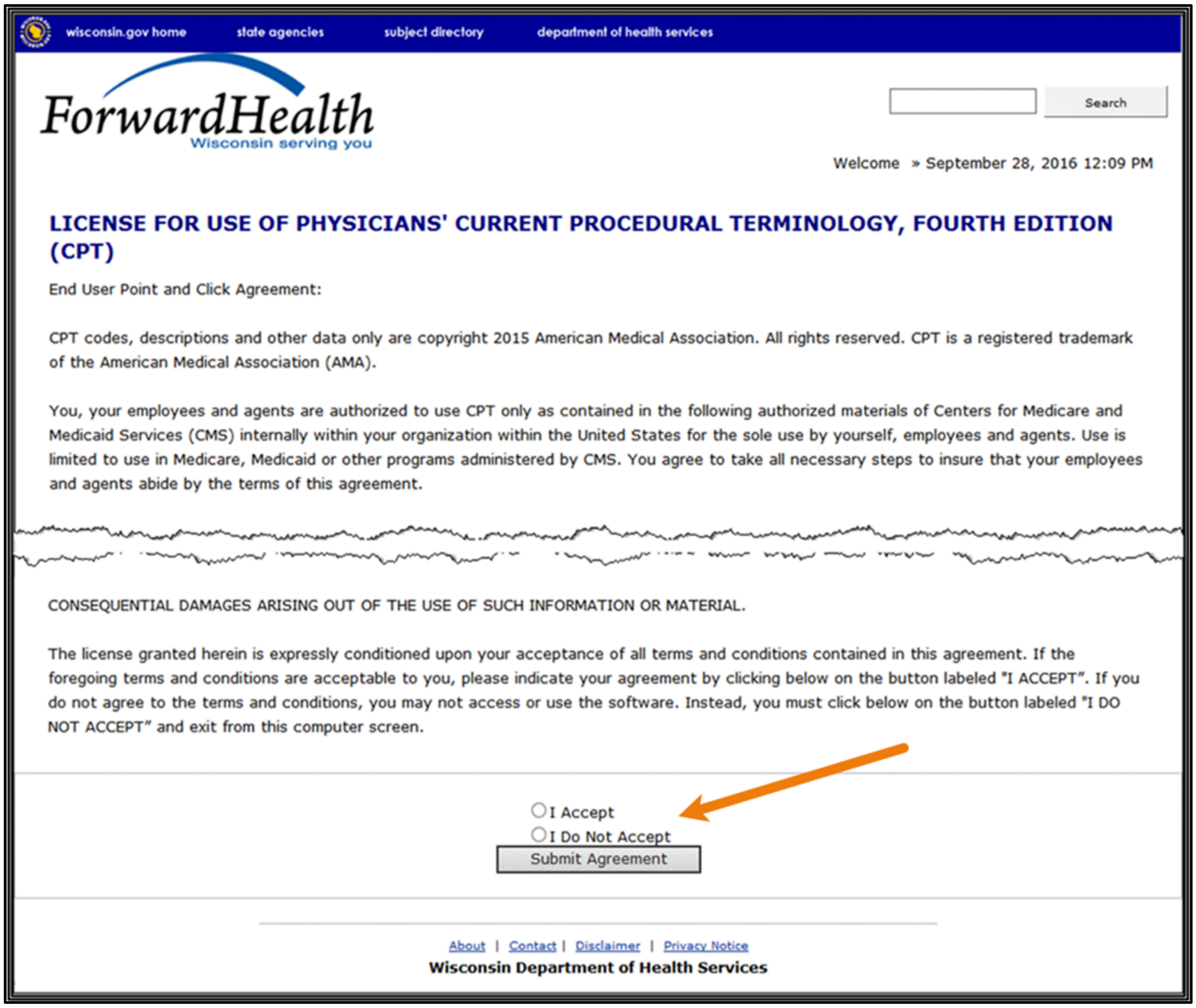


Figure 22 End User Point and Click License Agreements

11. 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 area of the Portal.

12. The user's secure Provider page will be displayed. Users will have access to the links located under the Home Page, Quick Links, and Electronic Visit Verification Links sections.

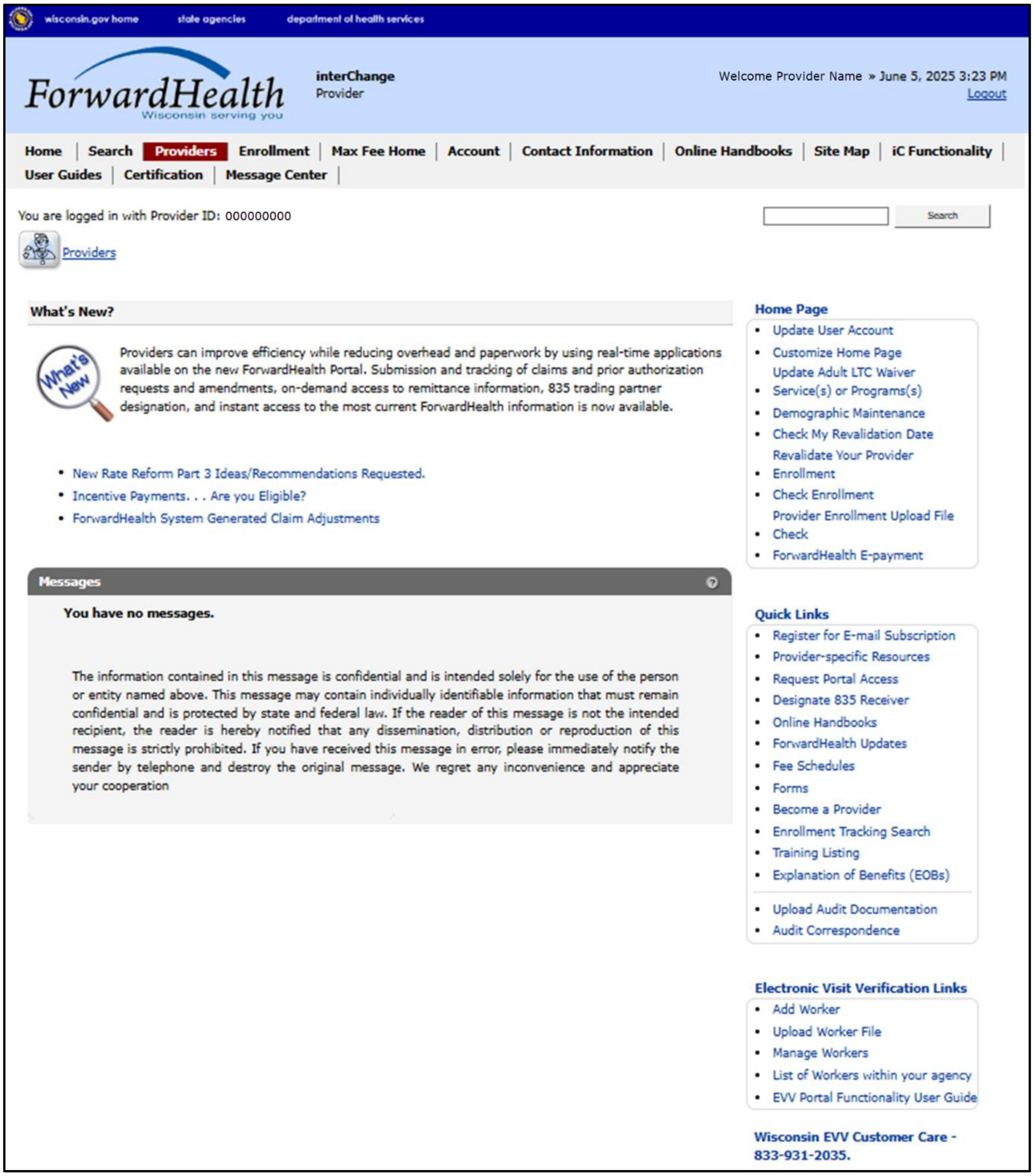


Figure 23 Secure Provider Page

4.2 Reset Password

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

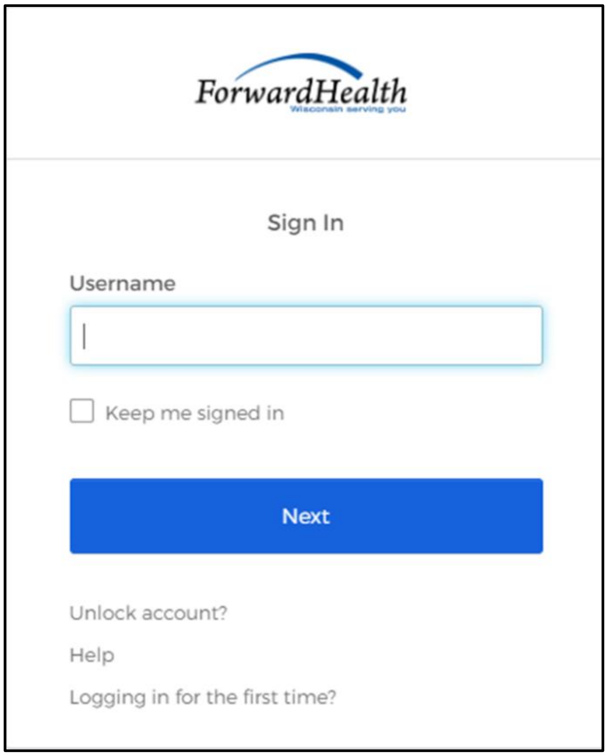


Figure 24 Sign-In Box

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

A Verify with your password box will be displayed.

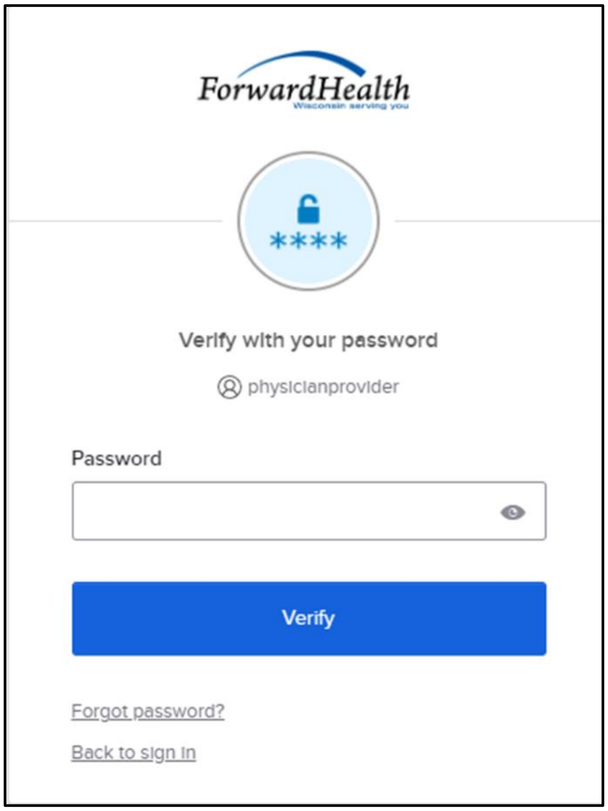


Figure 25 Verify With Your Password Box

5. Click **Forgot password?**

A Reset your password box will be displayed.

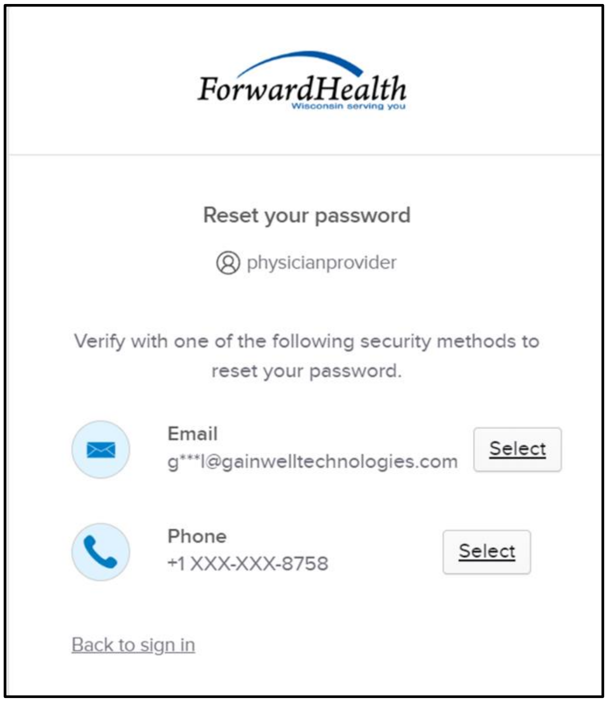


Figure 26 Reset Your Password Box

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.

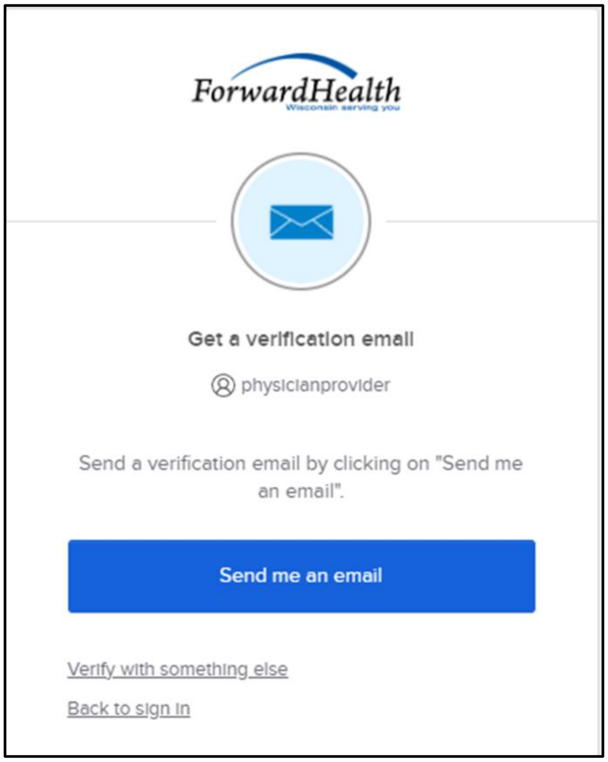


Figure 27 Get A Verification Email

  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.

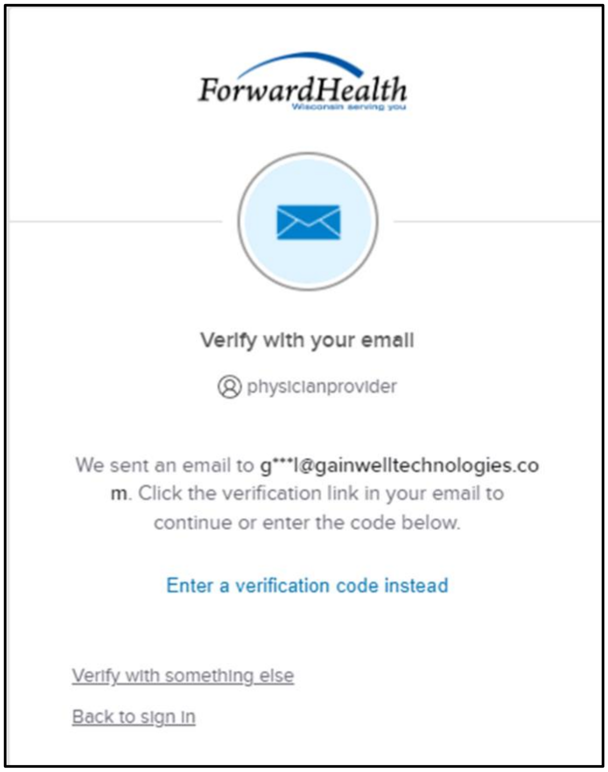


Figure 28 Verify With Your Email Box

c. Proceed to Step 7.

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

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

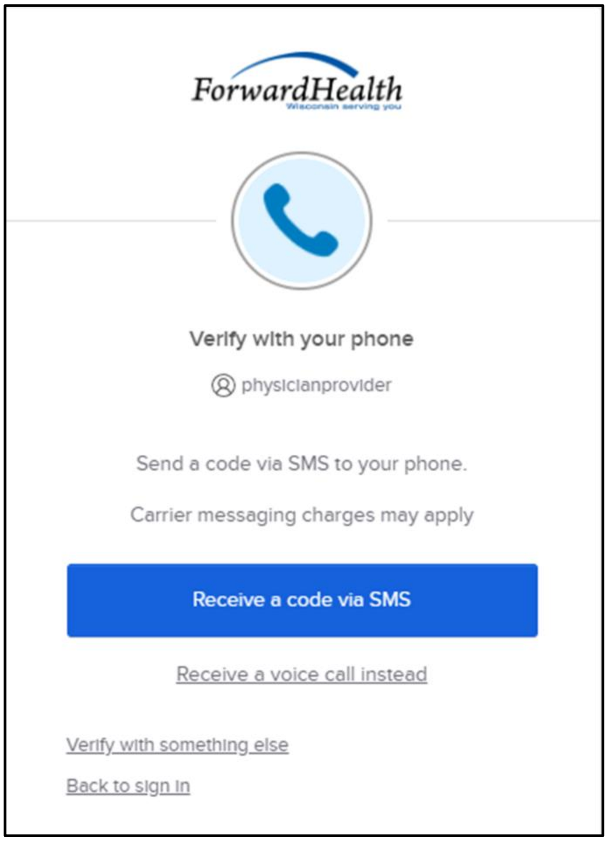


Figure 29 Verify With Your Phone Box

  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.

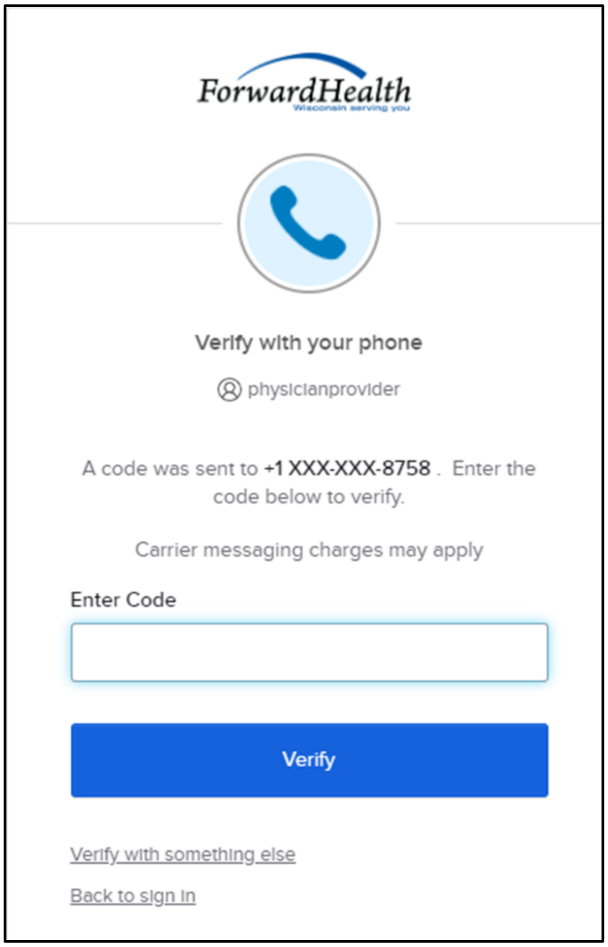


Figure 30 Verify With Your Phone Box

c. Enter the code that was sent.

d. Click **Verify**.

A Get a verification email box will be displayed.

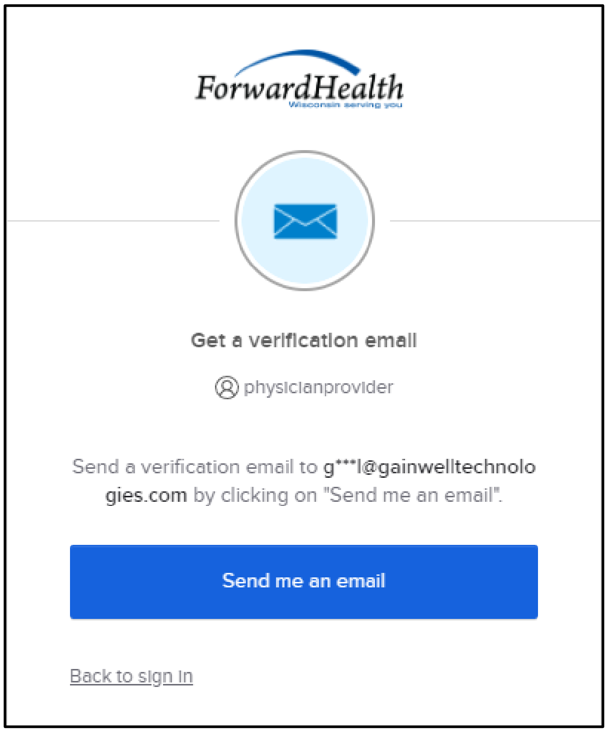


Figure 31 Get A Verification Email Box

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

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

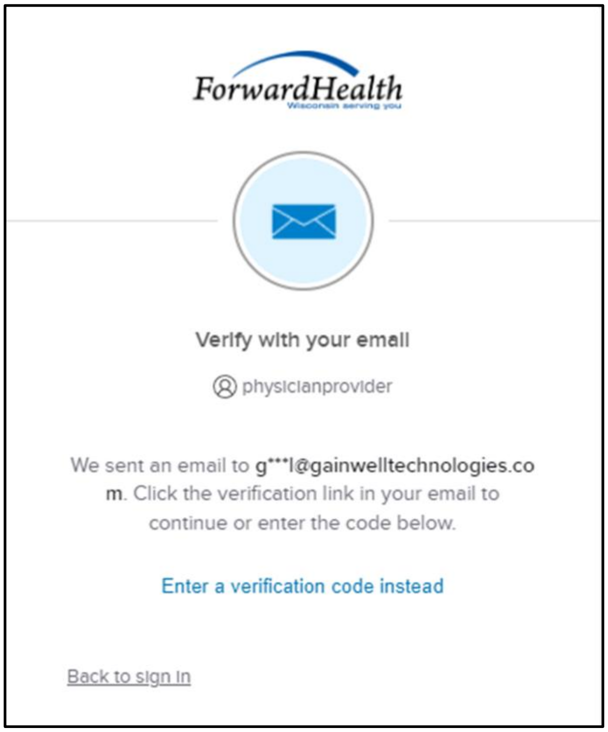


Figure 32 Verify With Your Email Box

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

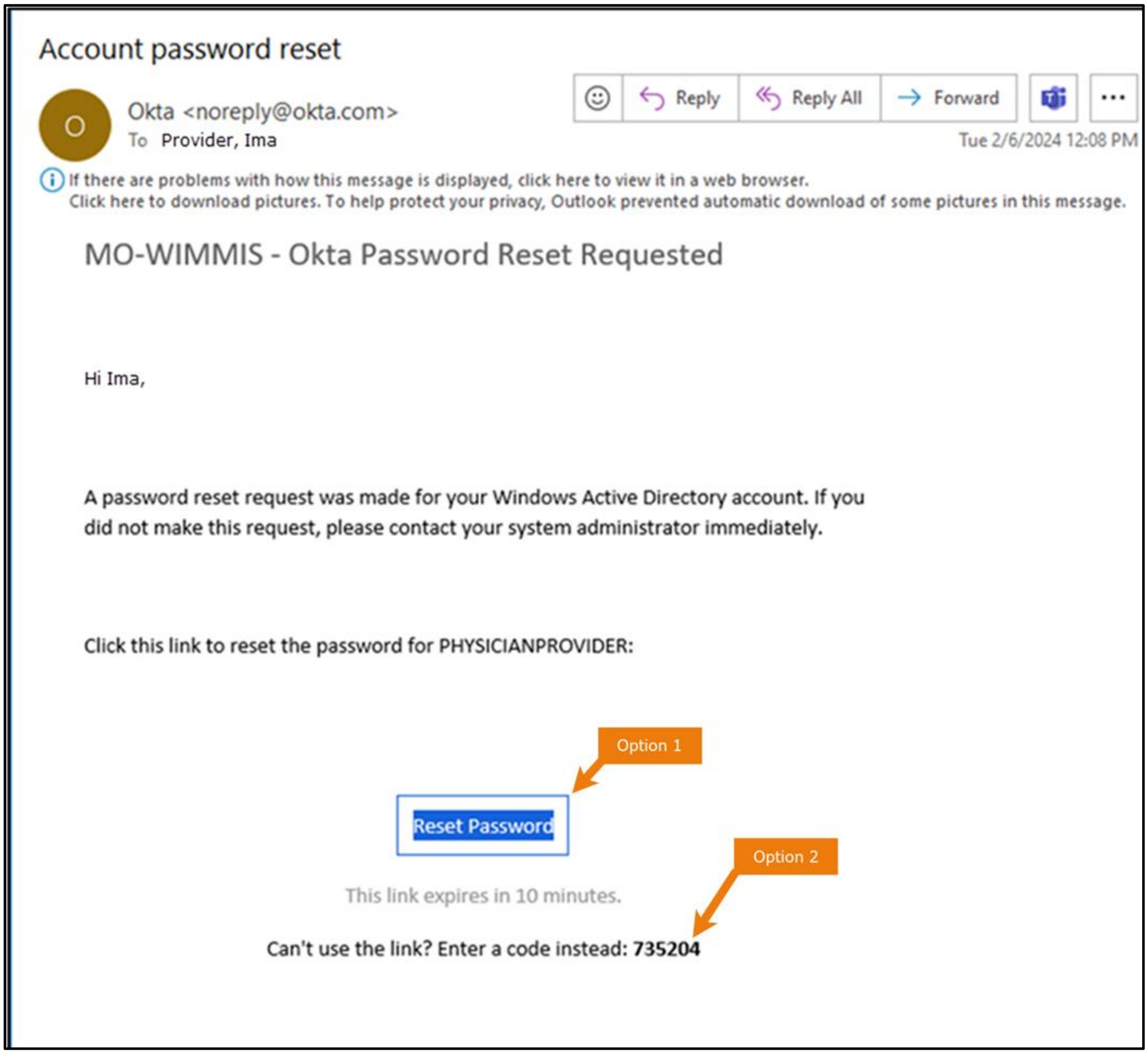


Figure 33 Account Password Reset Email

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.

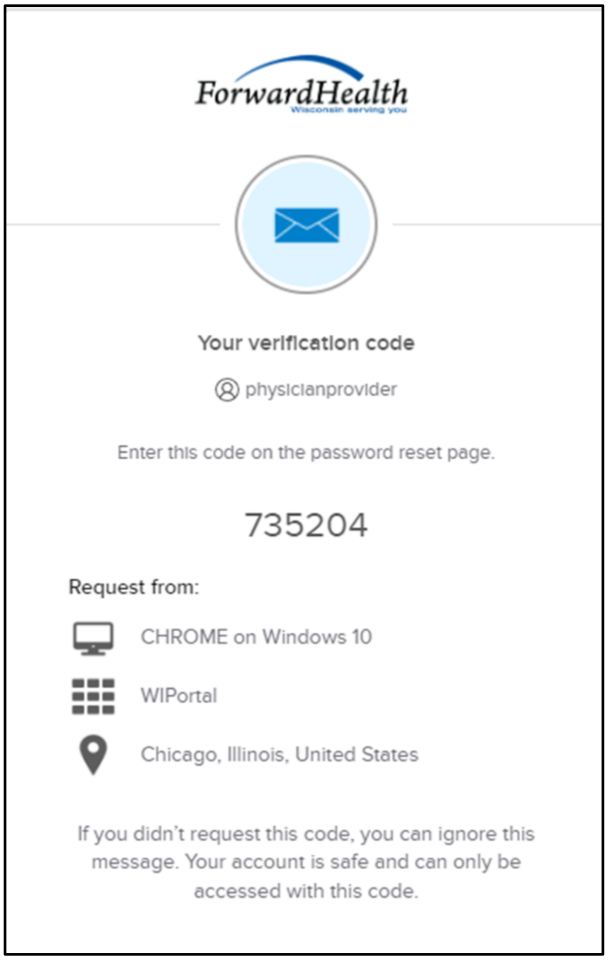


Figure 34 Verification Code Box

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**.

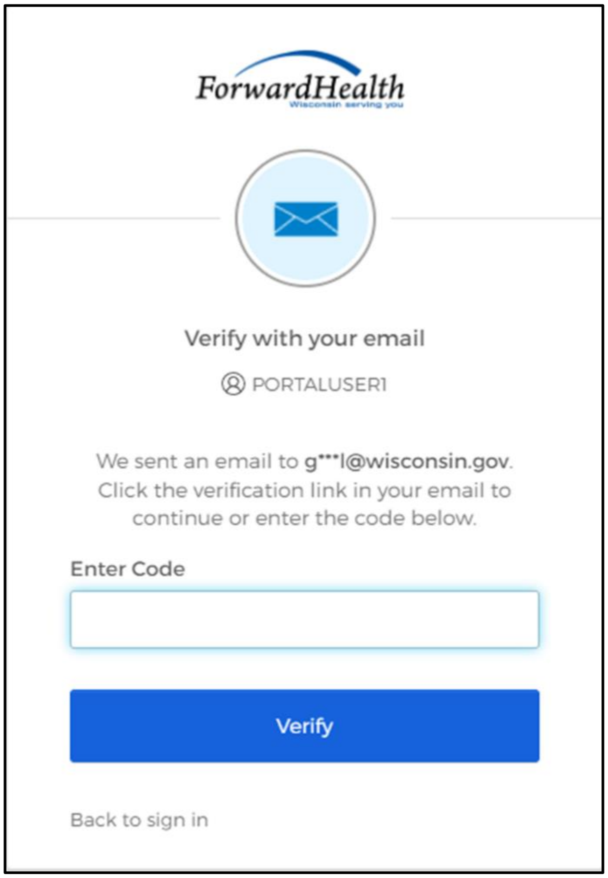


Figure 35 Verify With Your Email Box

The Reset your Okta password box will be displayed.

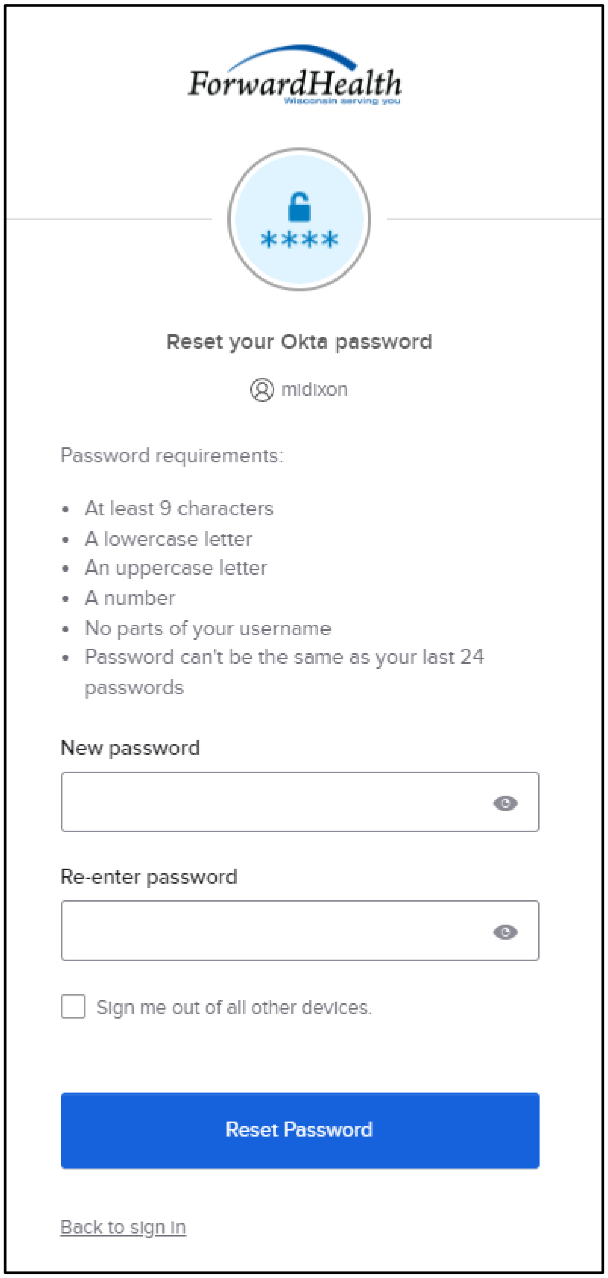


Figure 36 Reset Your Okta Password Box

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.

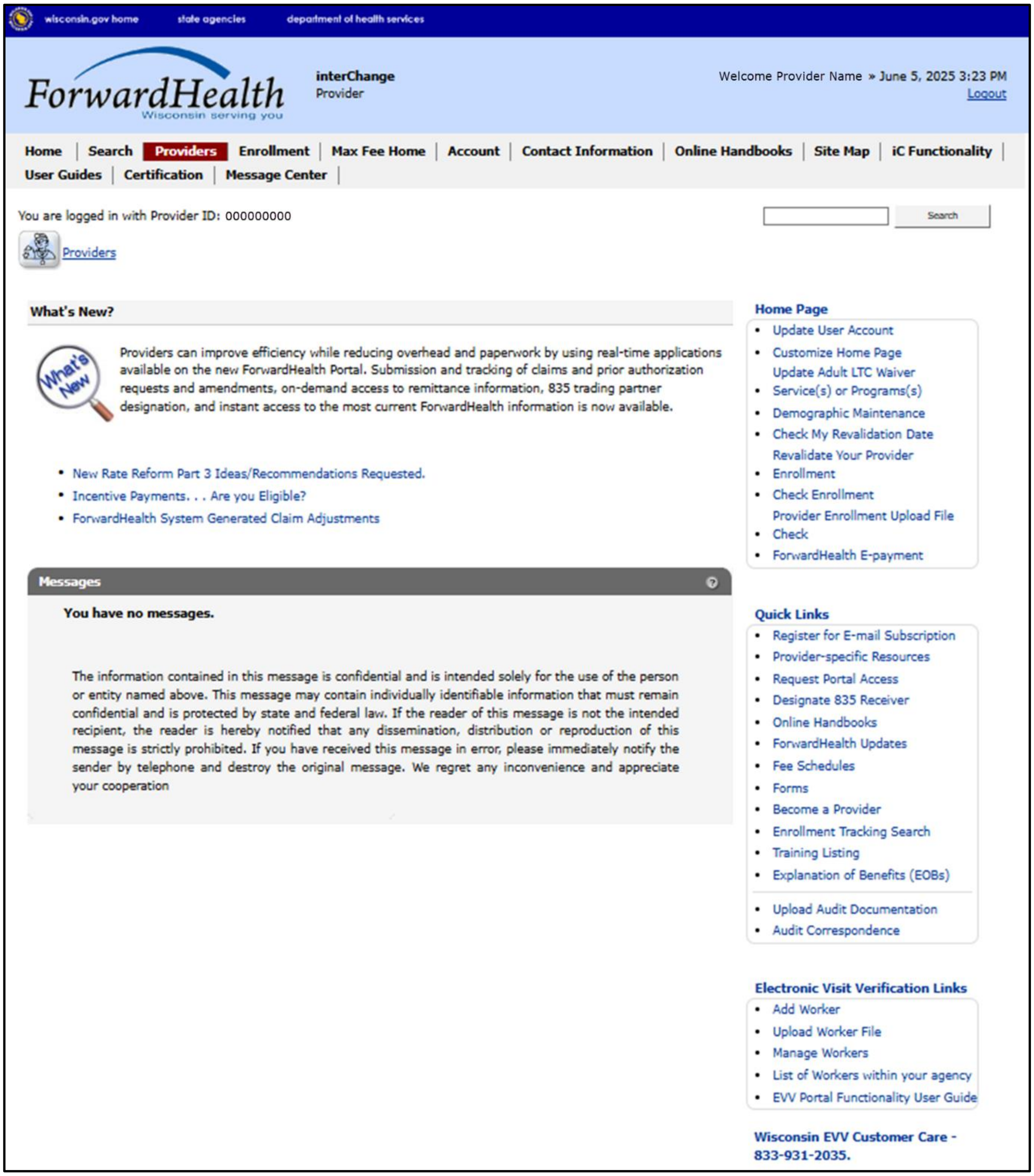


Figure 37 Secure Portal Page

4.3 Unlocking An Account

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

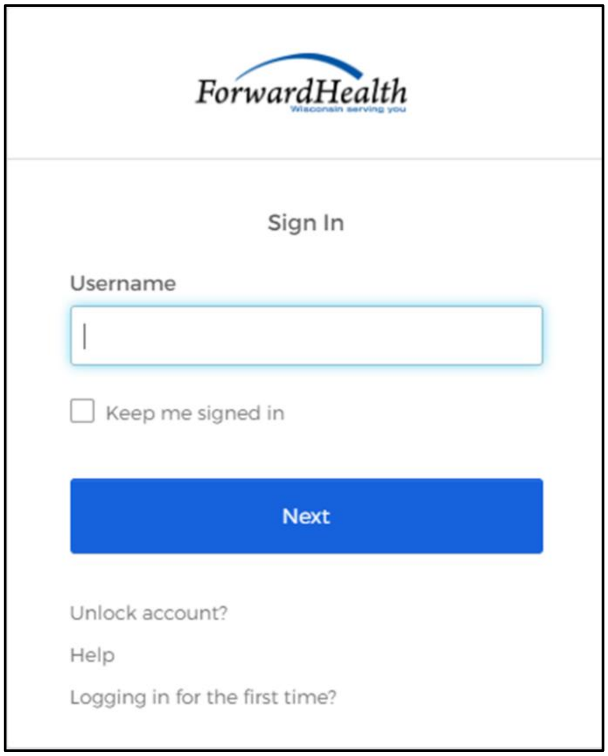


Figure 38 Sign In Box

3. Click **Unlock account?**

An Unlock account box will be displayed.

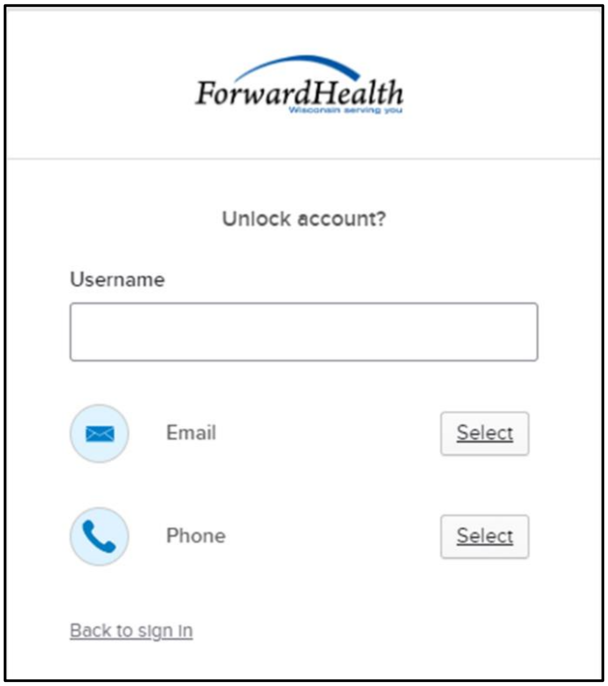


Figure 39 Unlock Account Box

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.

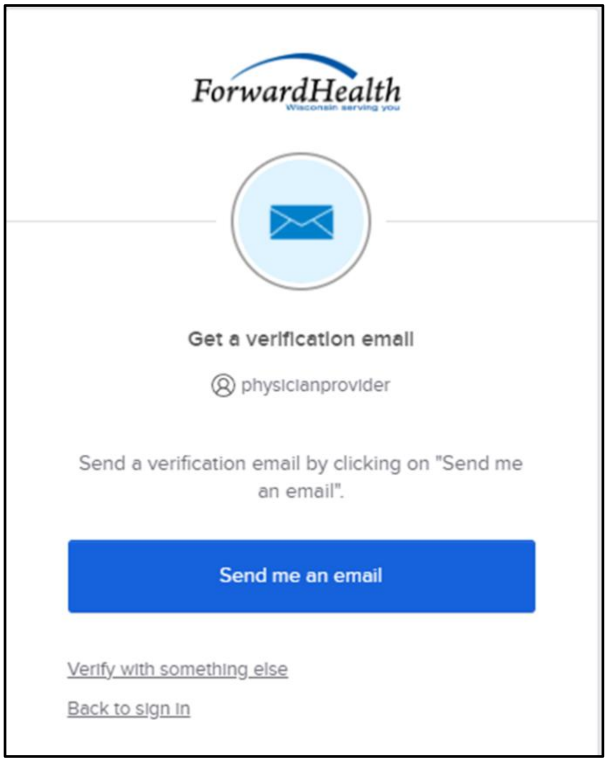


Figure 40 Get a Verification Email Box

  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.

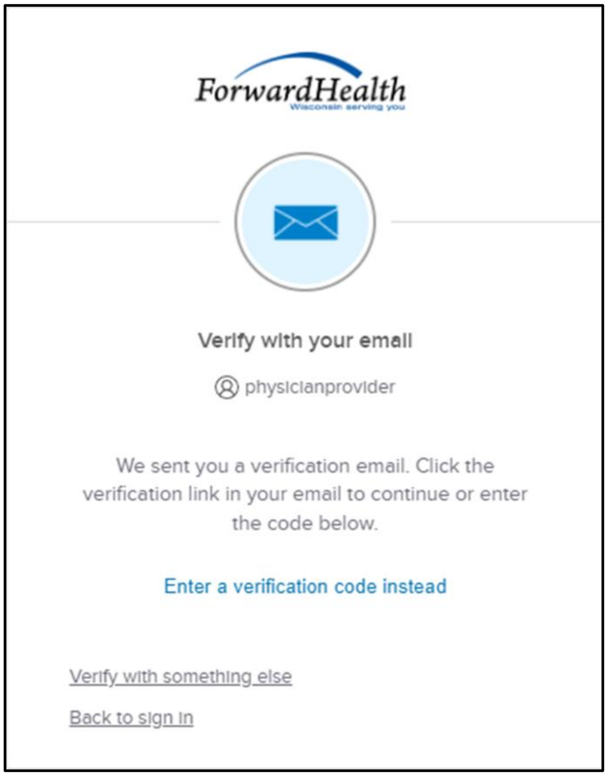


Figure 41 Verify With Your Email Box

c. Proceed to Step 6.

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

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

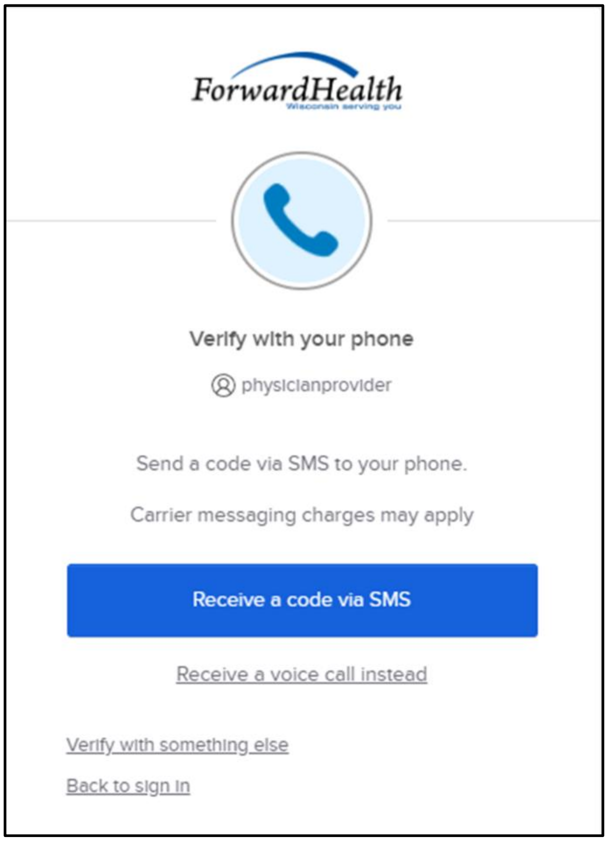


Figure 42 Verify With Your Phone Box

  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.

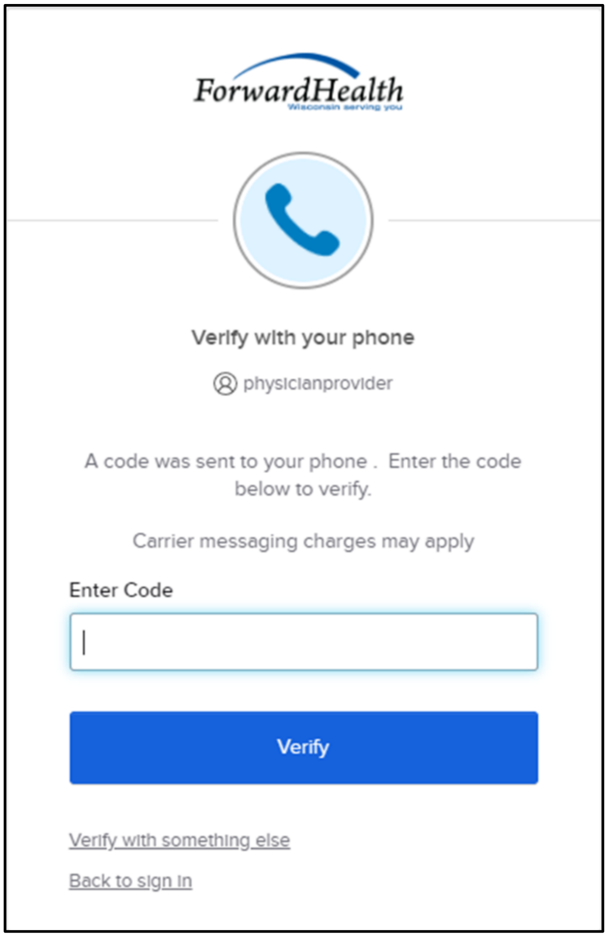


Figure 43 Verify With Your Phone Box

c. Enter the code that was sent.

d. Click **Verify**.

A Get a verification email box will be displayed.

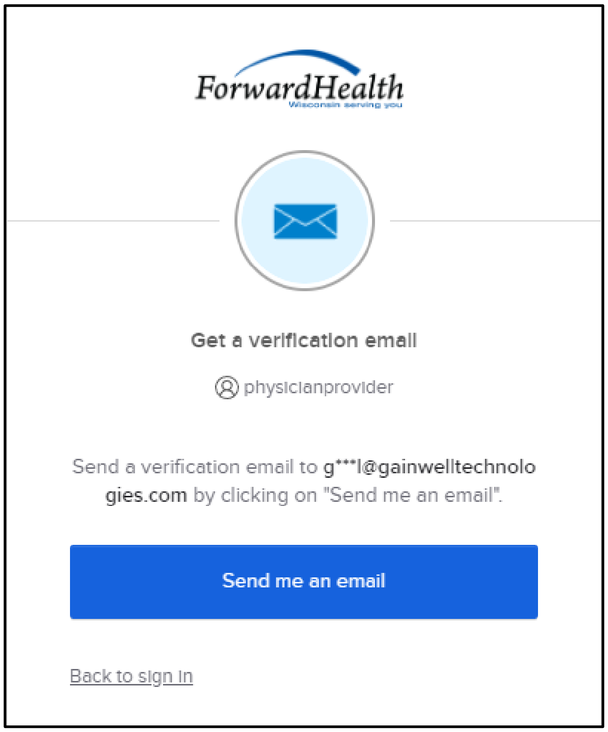


Figure 44 Get a Verification Email Box

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

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

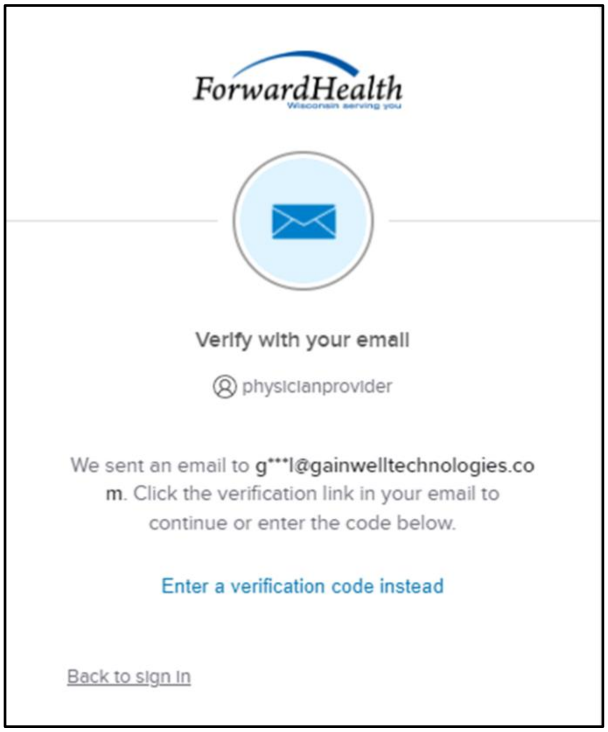


Figure 45 Verify With Your Email Box

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

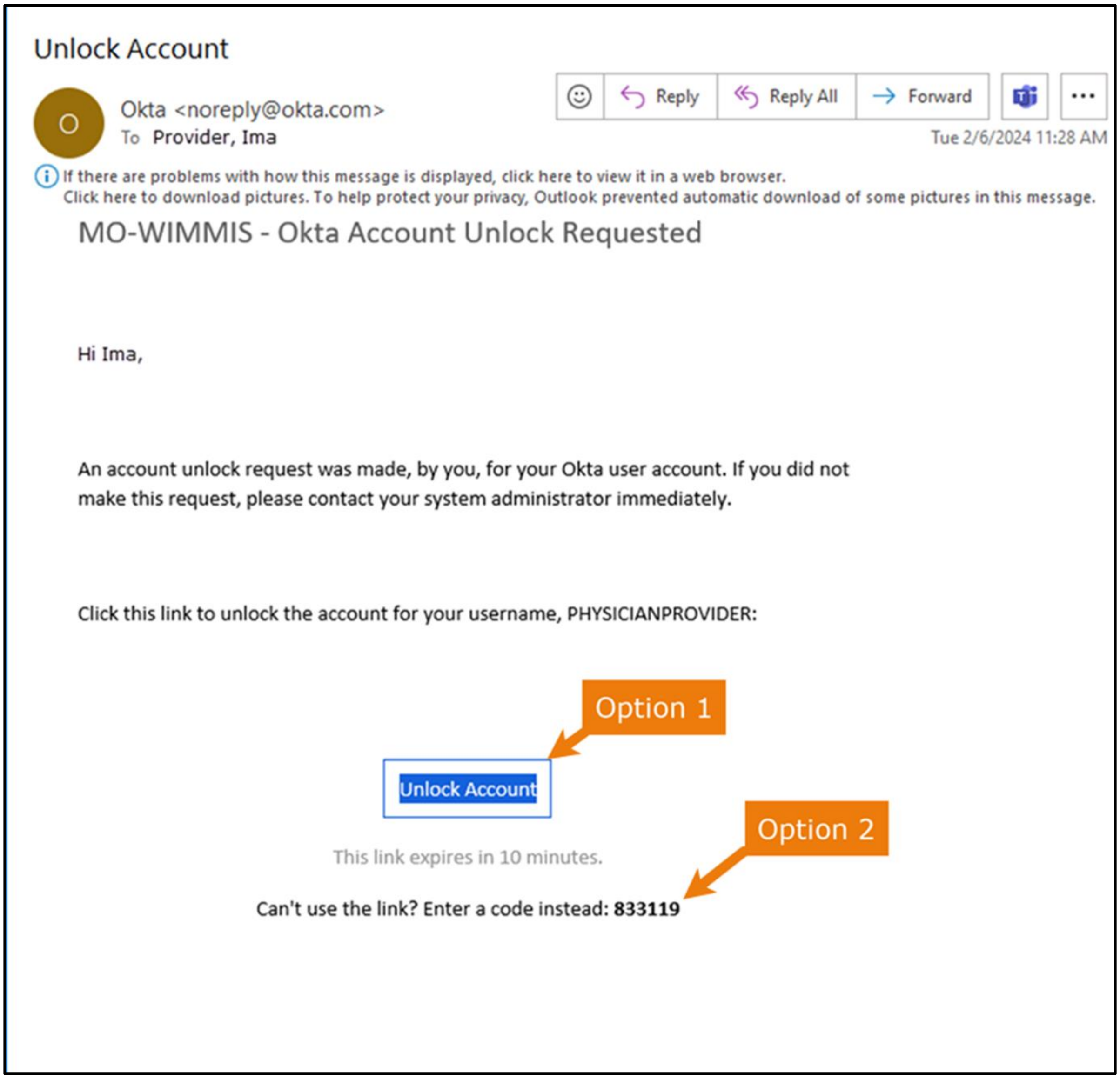


Figure 46 One-Time Verification Code Email

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.

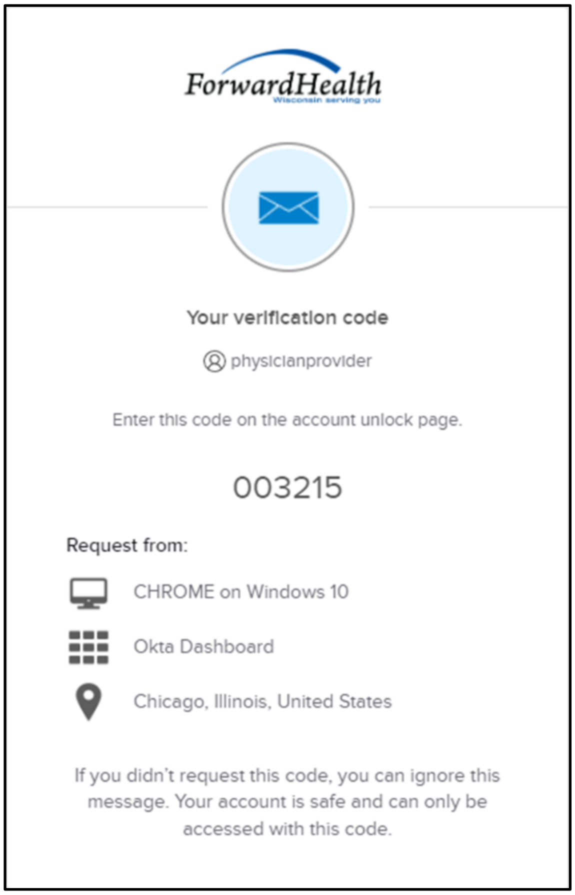


Figure 47 Verification Code Box

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.

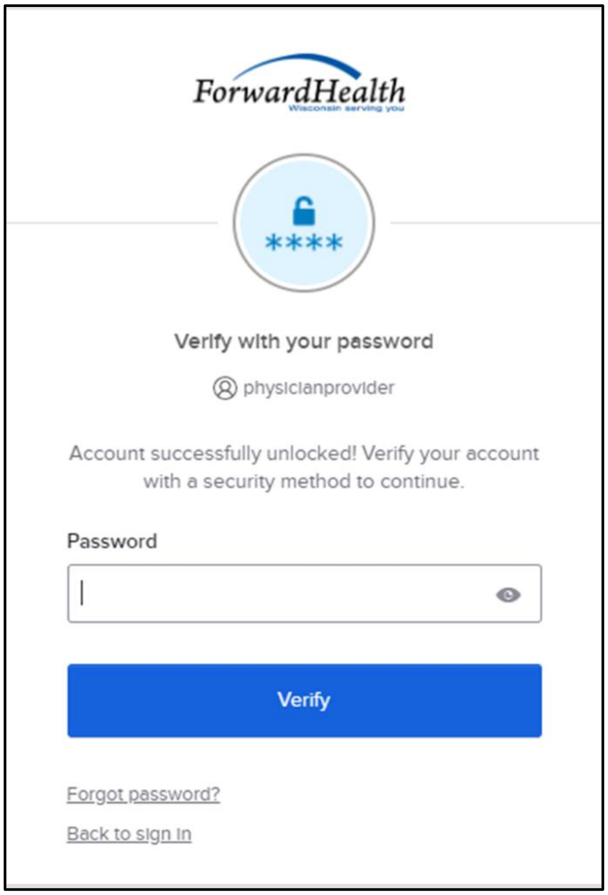


Figure 48 Verification Code Box

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

4.4 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 the following functions in the secure Portal:

    a. Home

    b. Search

    c. Electronic Visit Secure Home

d. Account

e. User Guides

f. Online Handbook

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 administrative 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. The functionality of the clerk administrative account includes the following:

a. Add Worker

b. Upload Worker

c. Manage Worker

d. List of Workers Within Your Agency

e. EVV Demographic Maintenance

f. EVV Portal User Guide

- *Clerk 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. Clerk accounts can also delete and manage clerk accounts under their account security.

5 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 by the administrator or clerk administrator.

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.

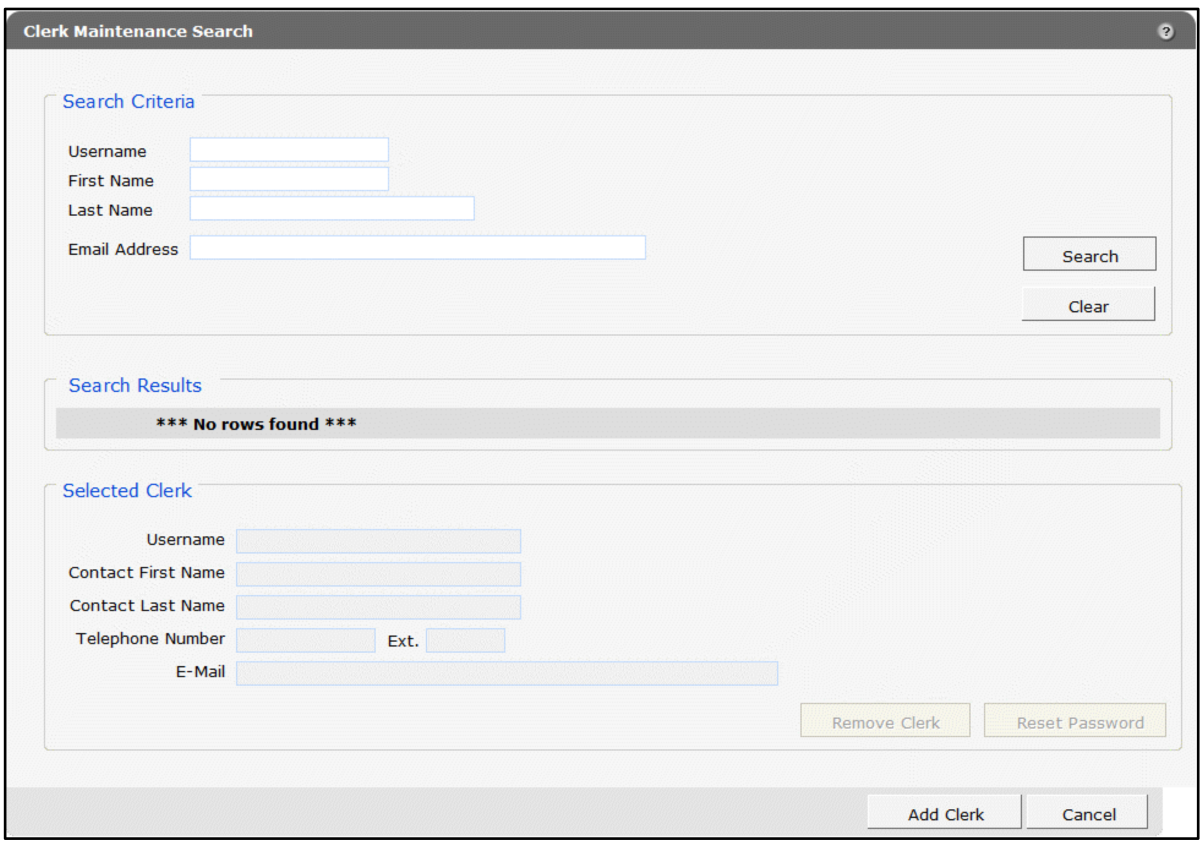


Figure 49 Clerk Maintenance Search Panel

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.

5.1 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.

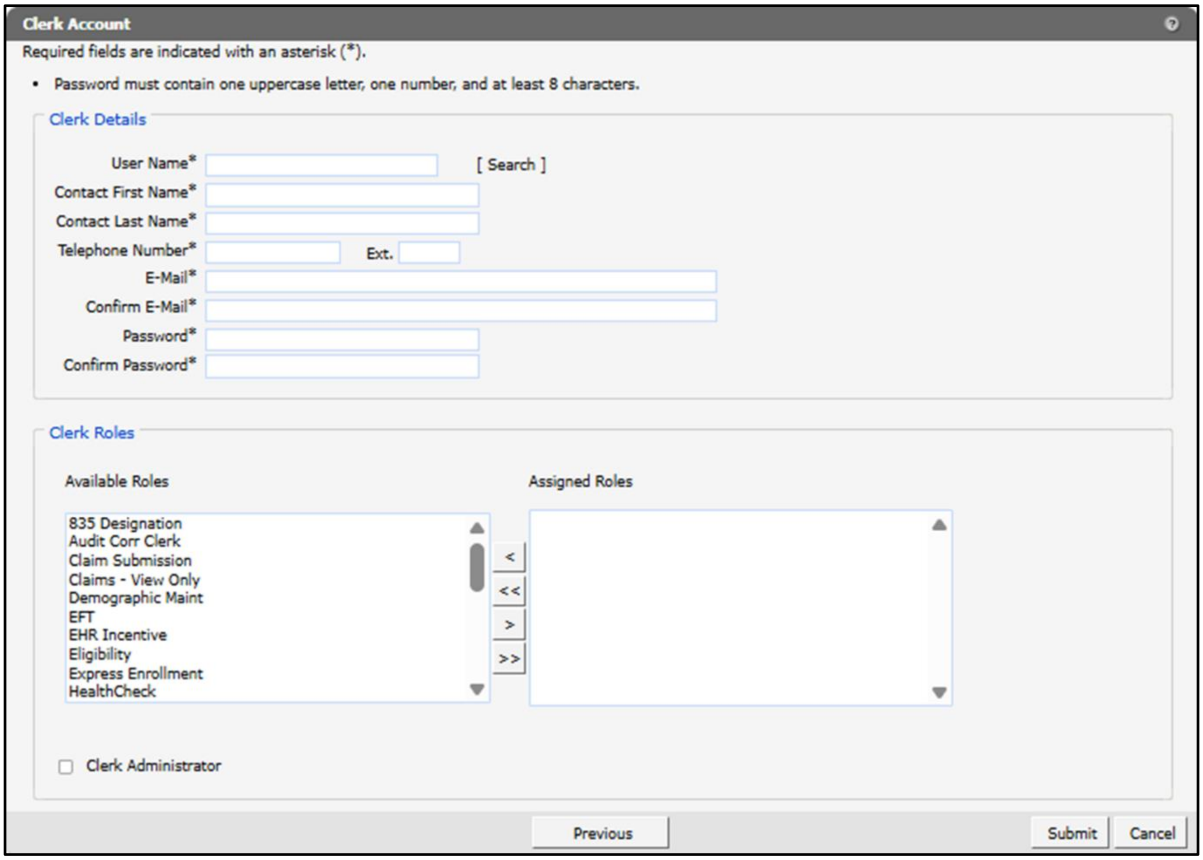


Figure 50 Clerk Account Panel

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 telephone 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 Username field. The User Name Search box will be displayed.

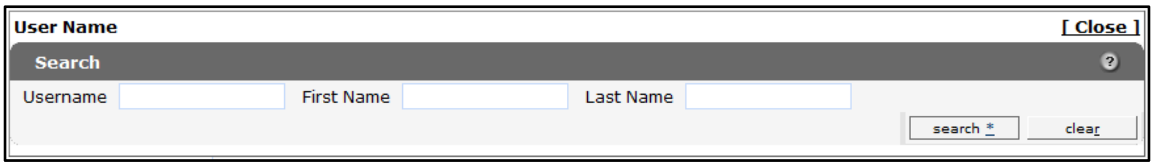


Figure 51 User Name Search Box

- 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.

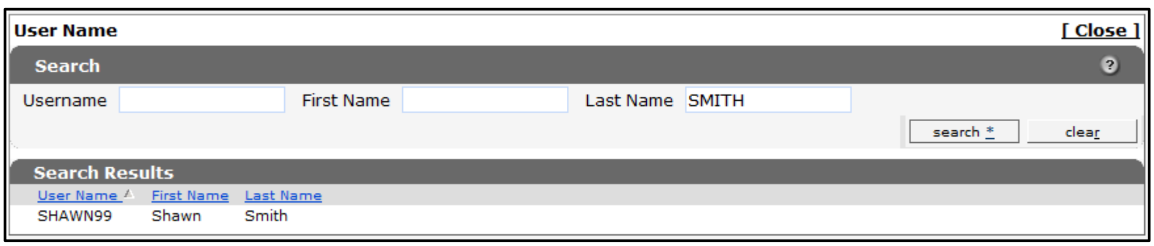


Figure 52 Search Results Section

- 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.

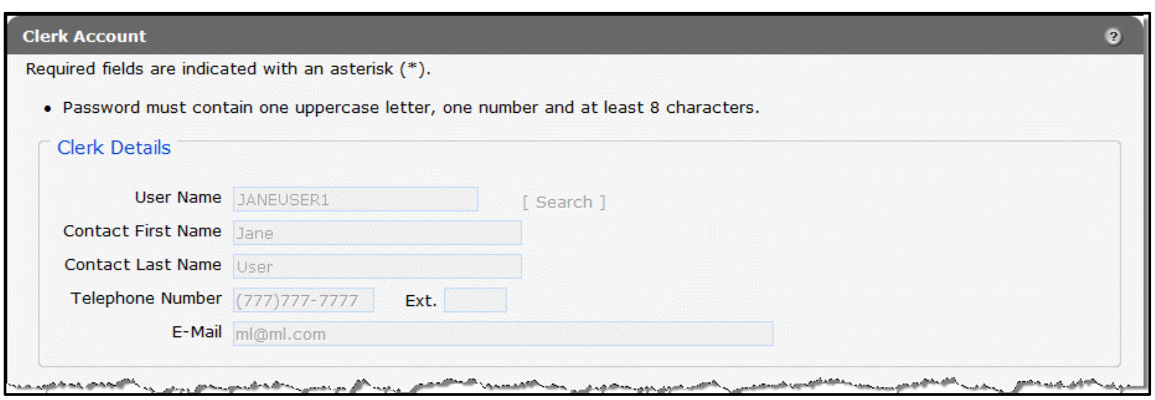


Figure 53 Clerk Account Information Auto-populated on Clerk Account Panel

2. Proceed to one of the following sections once clerk details have been entered or populated:
    - Step 2 of Section 5.3 Add a Role to a Clerk of this guide
    - Step 1 of Section 5.5 Assign a Clerk Administrator of this guide

5.2 Search for a Clerk

The Clerk Maintenance Search panel allows a user to select an existing clerk to associate to their agency.

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.

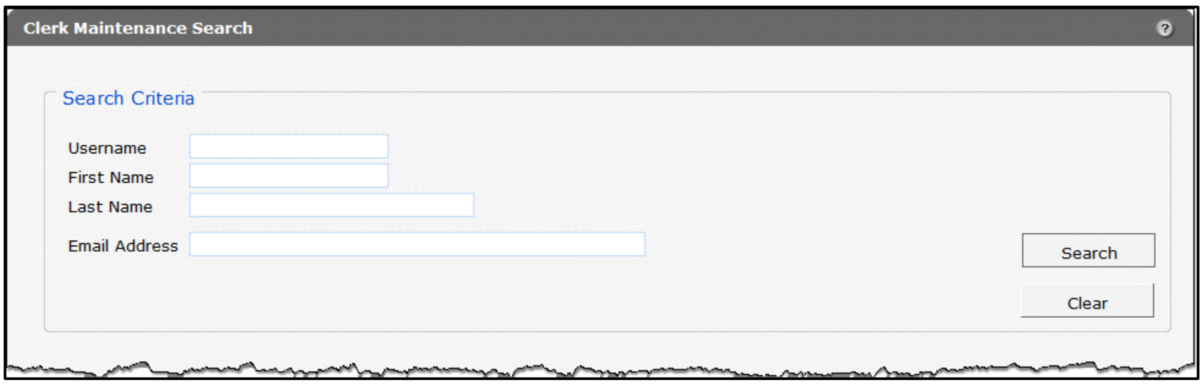


Figure 54 Search Criteria Section

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

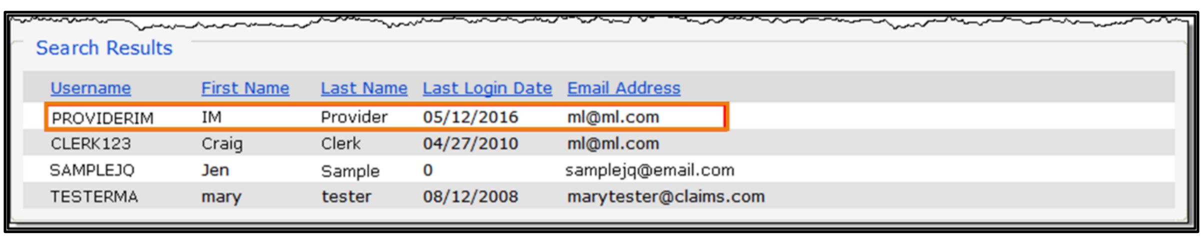


Figure 55 Search Results Section

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

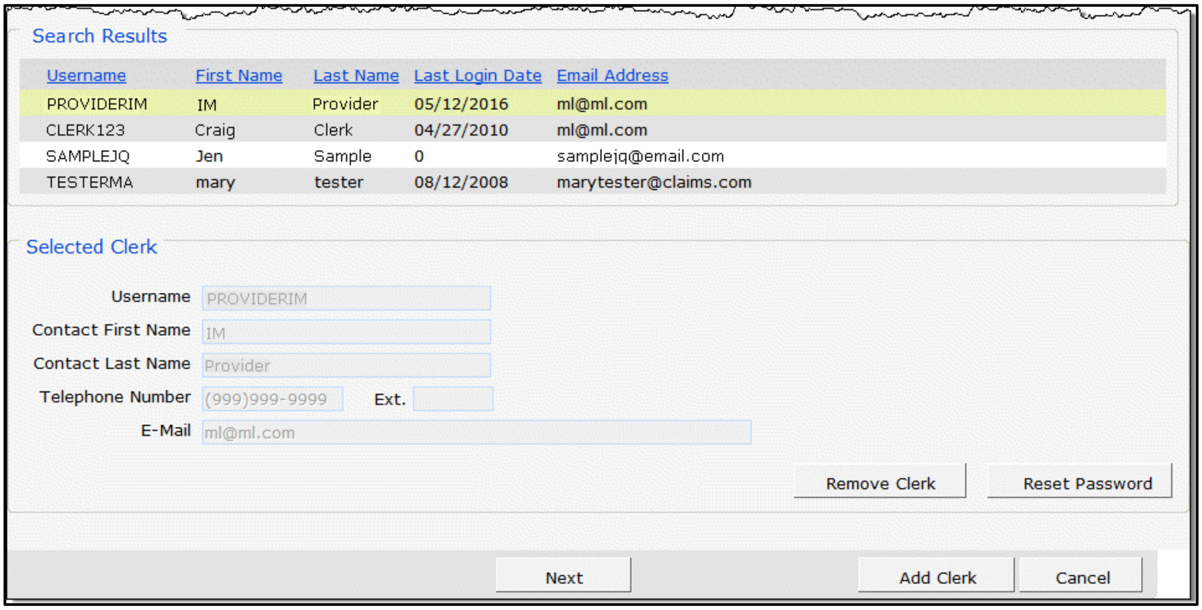


Figure 56 Search Results and Selected Clerk Sections

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

- Section 5.3 Add a Role to a Clerk
- Section 5.4 Remove a Role From a Clerk
- Section 5.5 Assign a Clerk Administrator
- Section 5.6 Reset a Clerk's Password
- Section 5.7 Delete a Clerk Account

5.3 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.

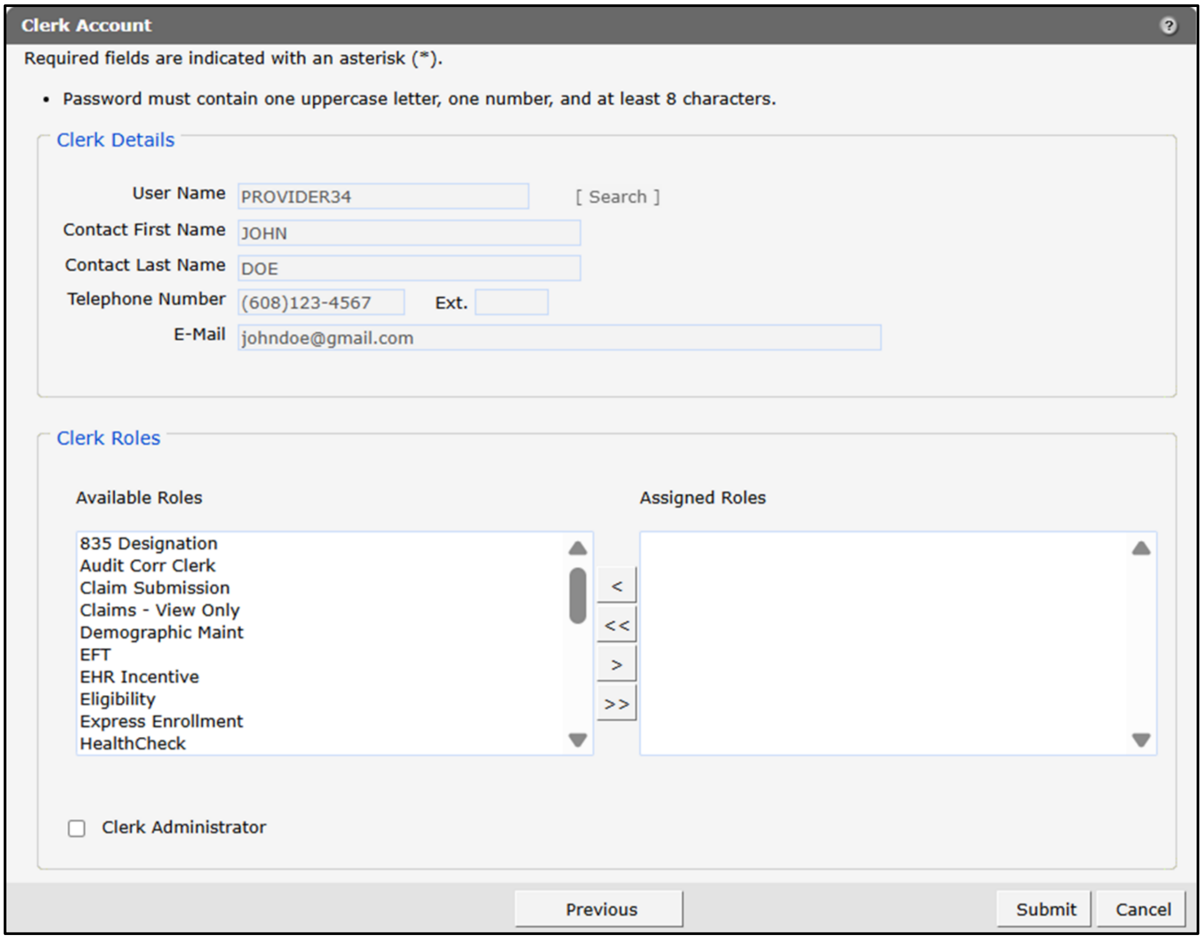


Figure 57 Clerk Account Panel

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. Note: The Provider EVV Clerk role is for EVV worker assignment. In addition to the EVV role, there are other long-term care waiver roles available to assign as necessary.

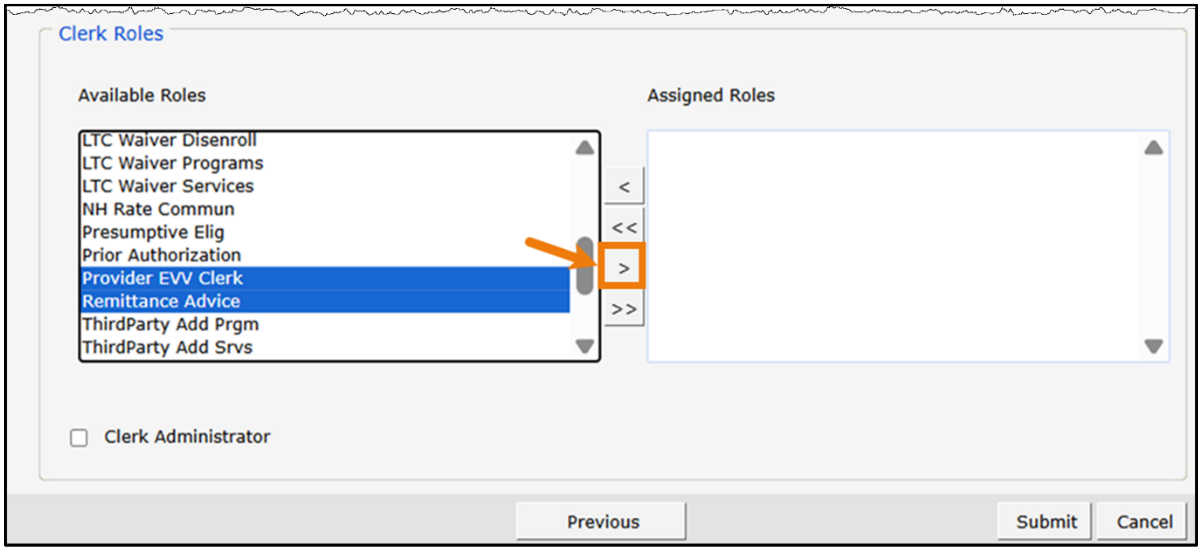


Figure 58 Clerk Roles Section With Available Roles

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

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

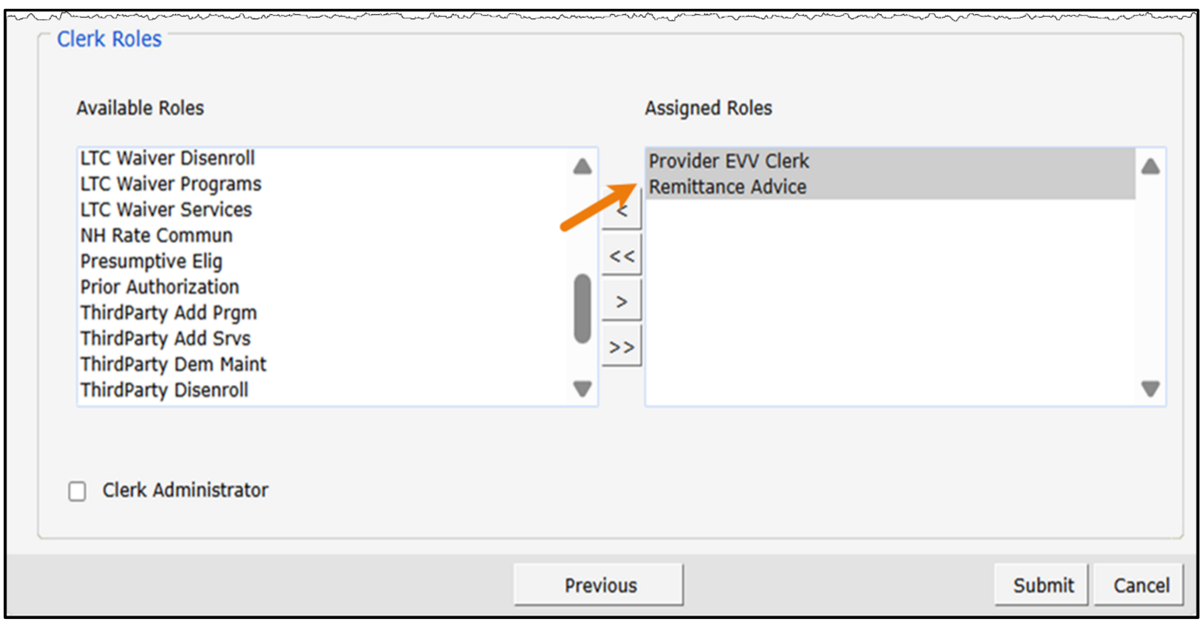


Figure 59 Clerk Roles Section With Assigned Roles

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

Figure 60 User Successfully Updated Message

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

5.4 Remove a Role From a Clerk

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

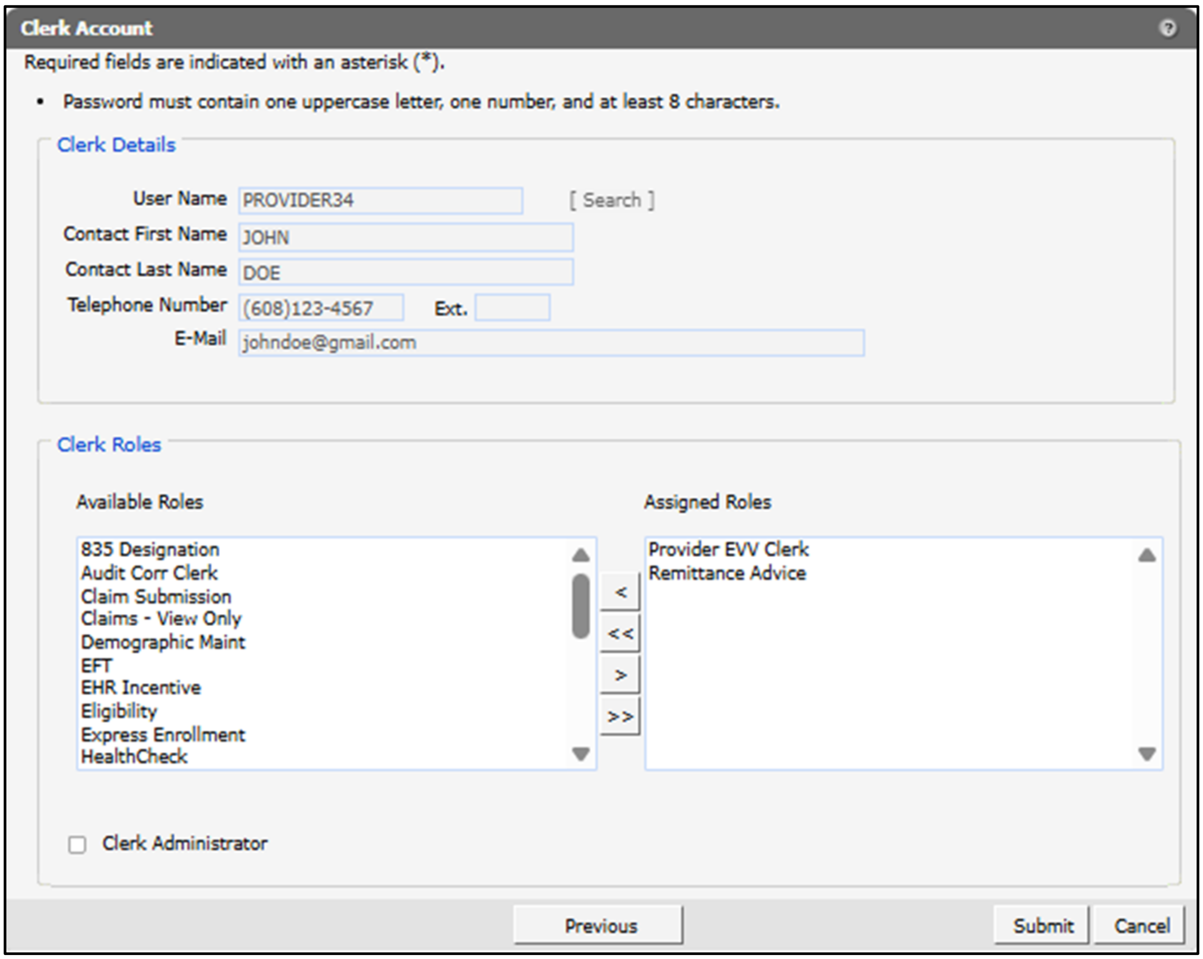


Figure 61 Clerk Account Panel

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.

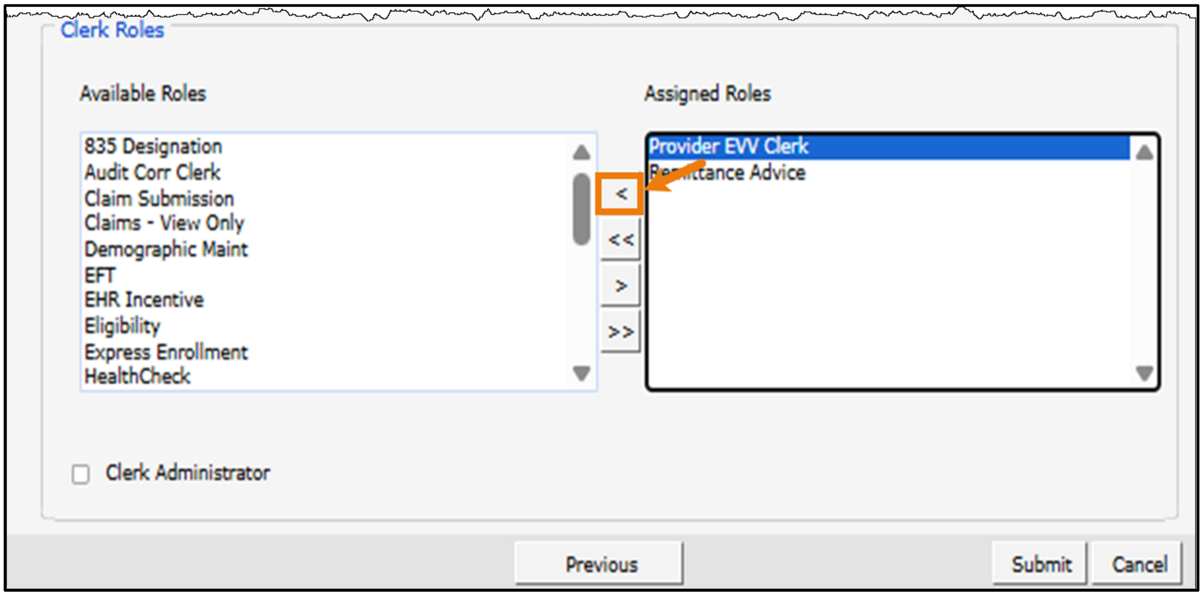


Figure 62 Clerk Roles Section With Assigned Roles

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 **<<.**

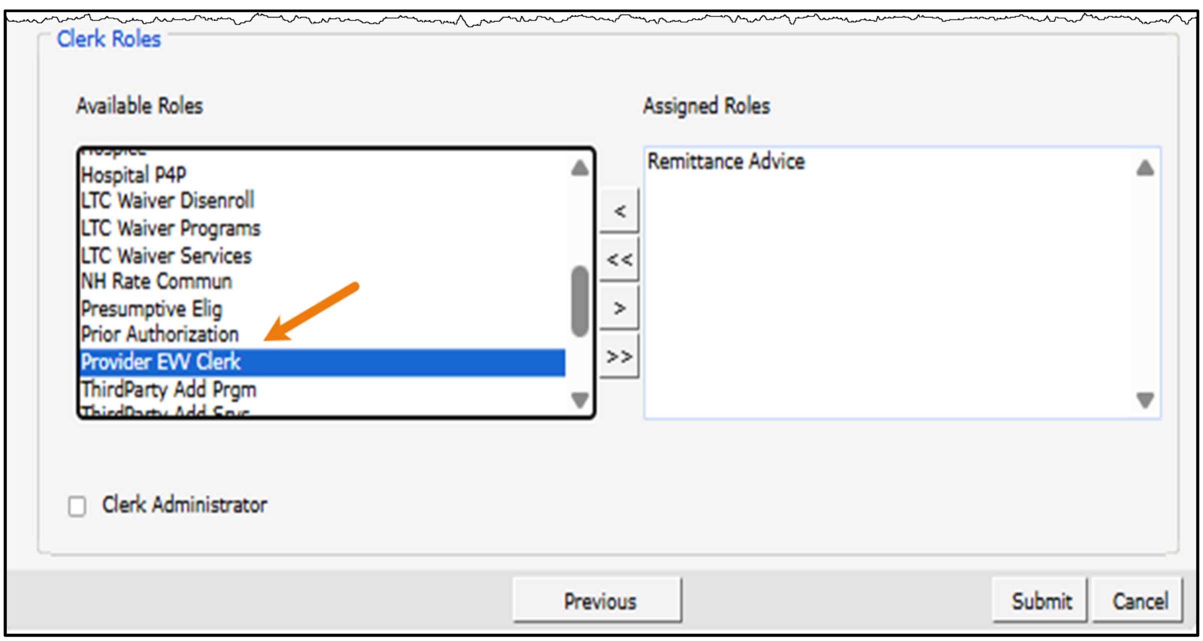


Figure 63 Clerk Roles Section With Role Removed

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

Figure 64 Confirmation Message

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

5.5 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.

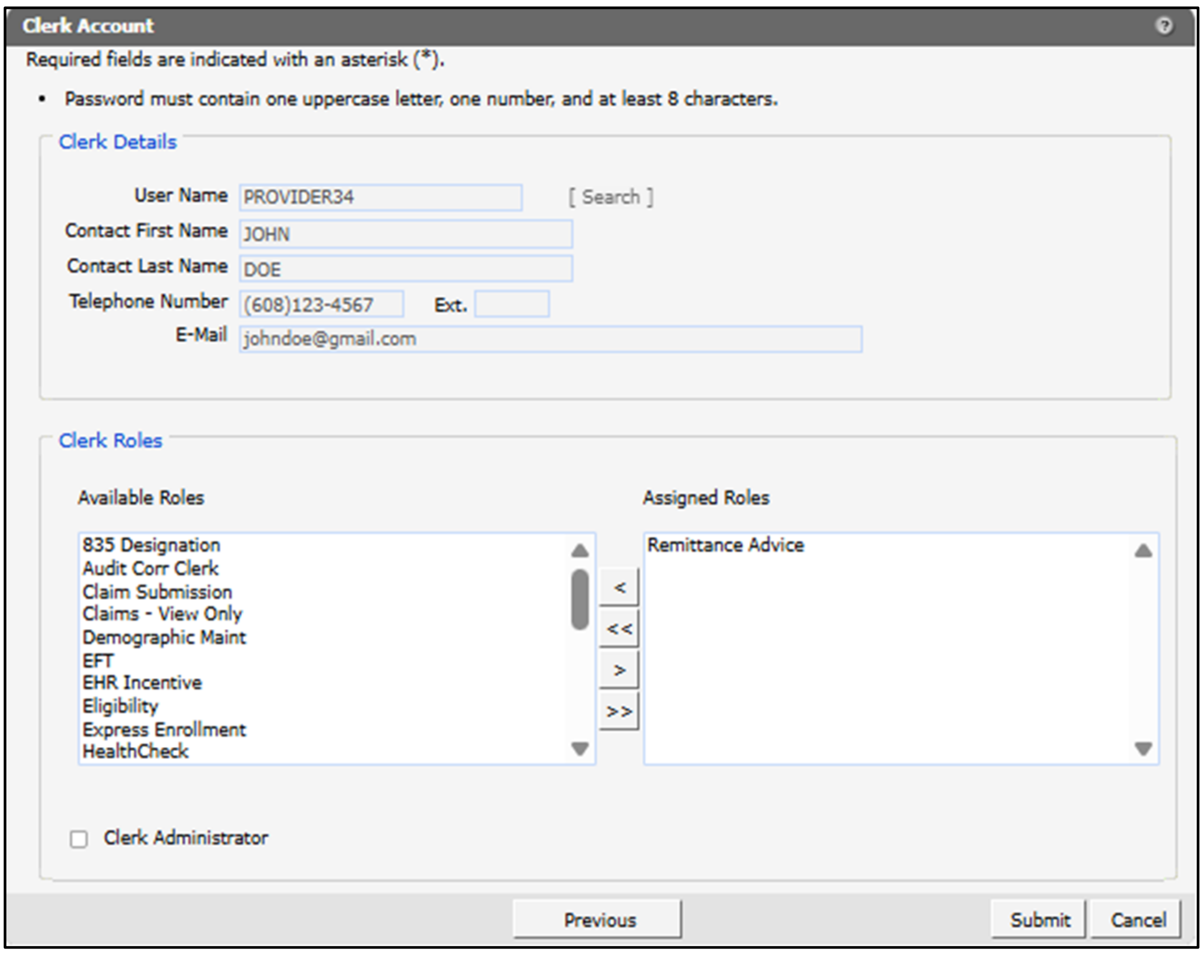


Figure 65 Clerk Account Panel

2. In the "Clerk Roles" section, check the Clerk Administrator box.

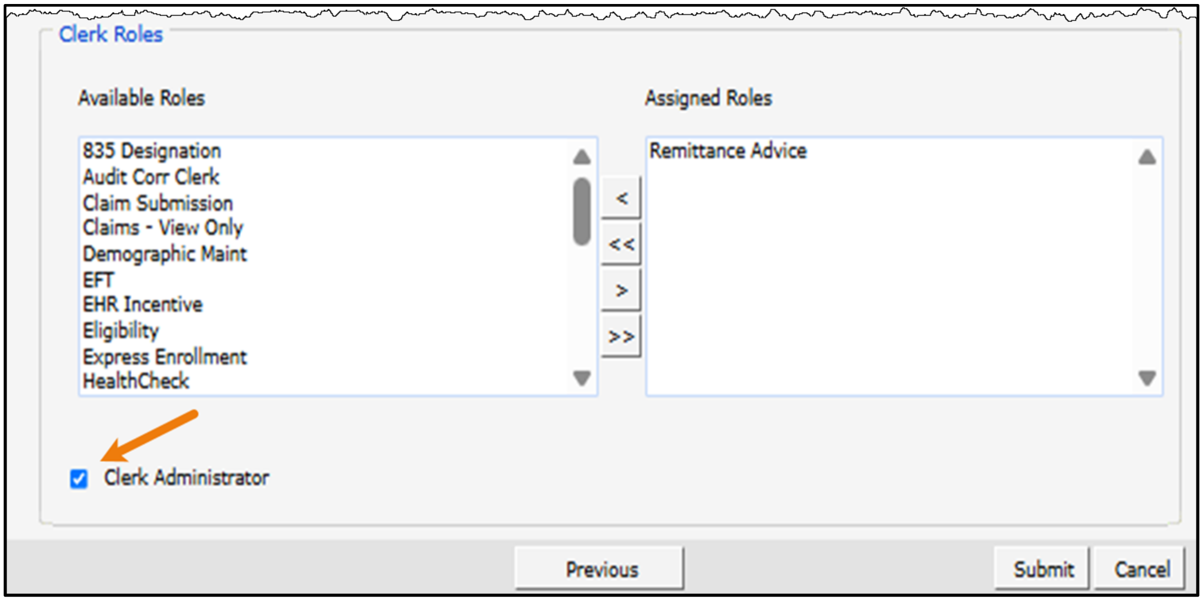


Figure 66 Clerk Roles Section With Clerk Administrator Checked

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

Figure 67 Confirmation Message

5.6 Reset a Clerk's Password

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

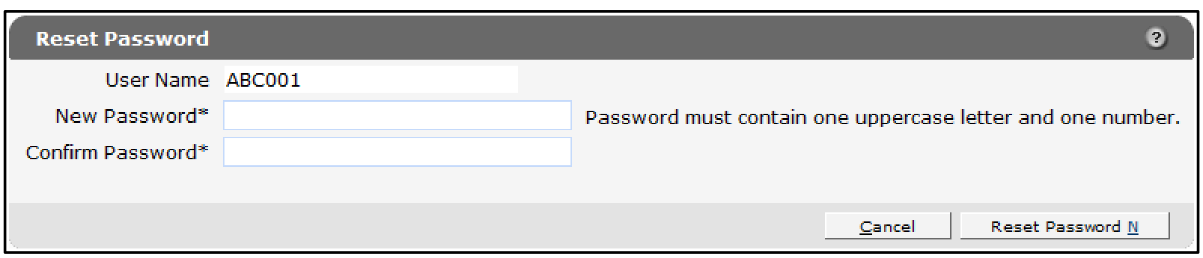


Figure 68 Reset Password Page

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.

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

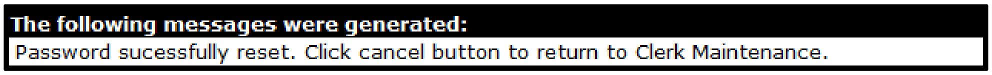


Figure 69 Confirmation Message

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.

5.7 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.

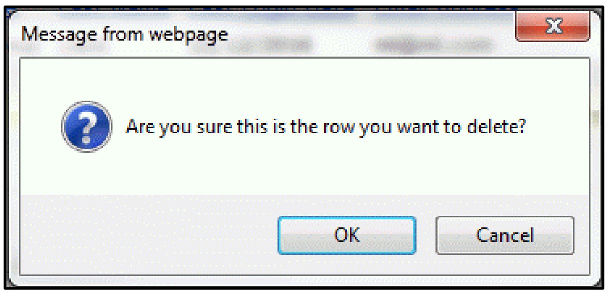


Figure 70 Dialog Box

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

Figure 71 Confirmation Message

5.8 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 forwardhealth.wi.gov/.

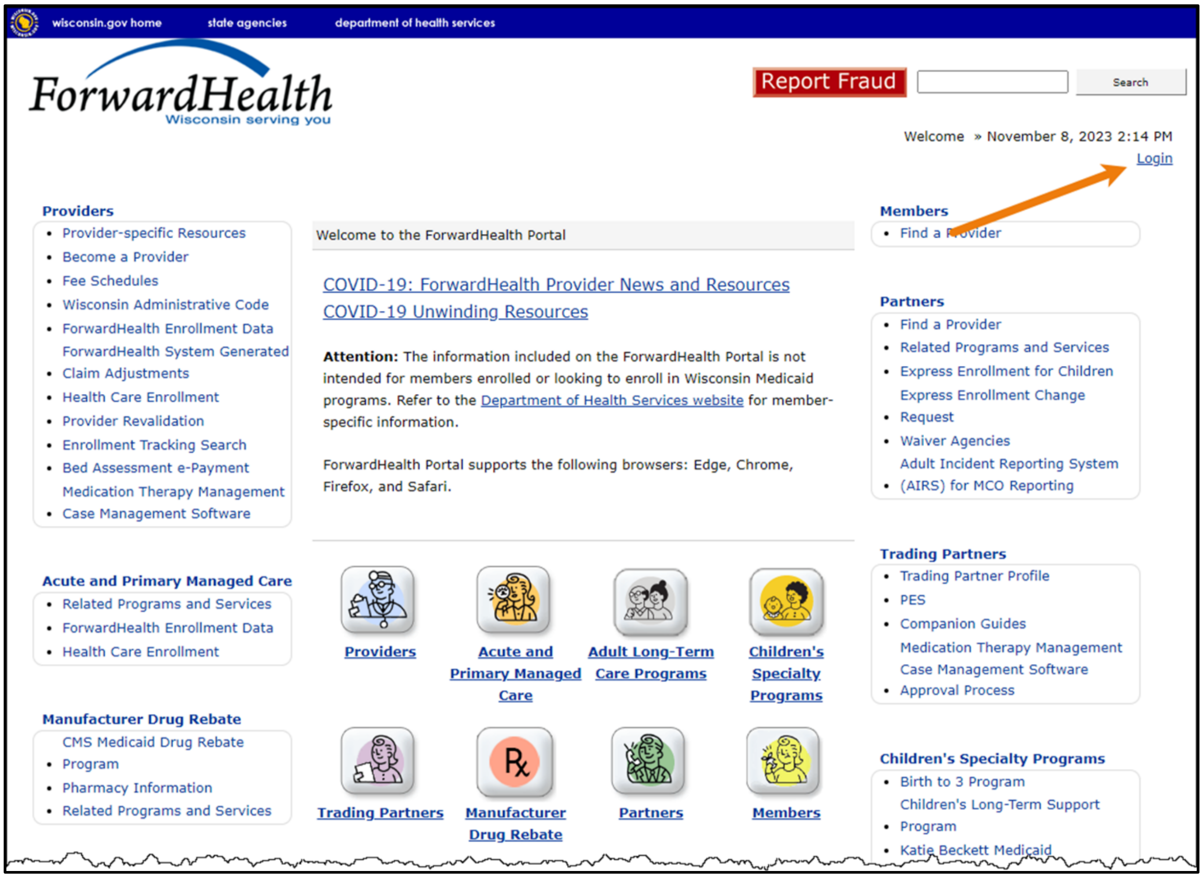


Figure 72 ForwardHealth Portal Page

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

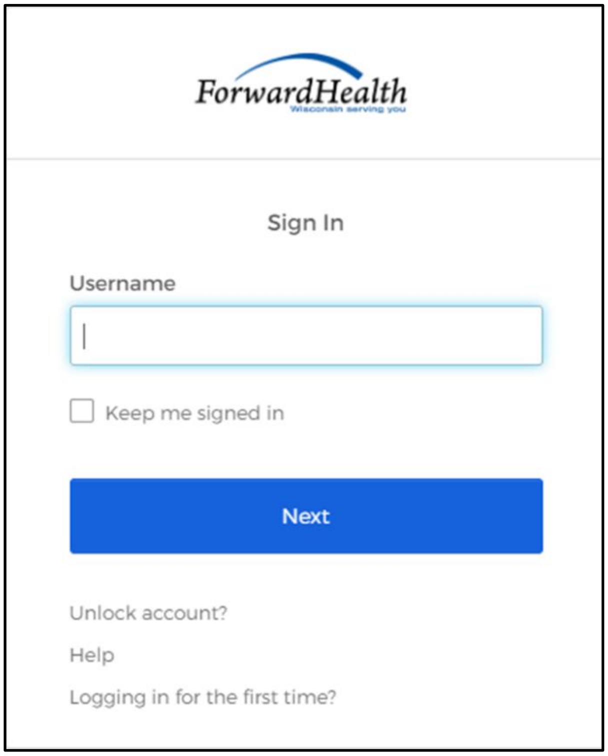


Figure 73 Sign In Box

3. Enter the user's username.

4. Click **Next**.

A Verify with your password box will be displayed.

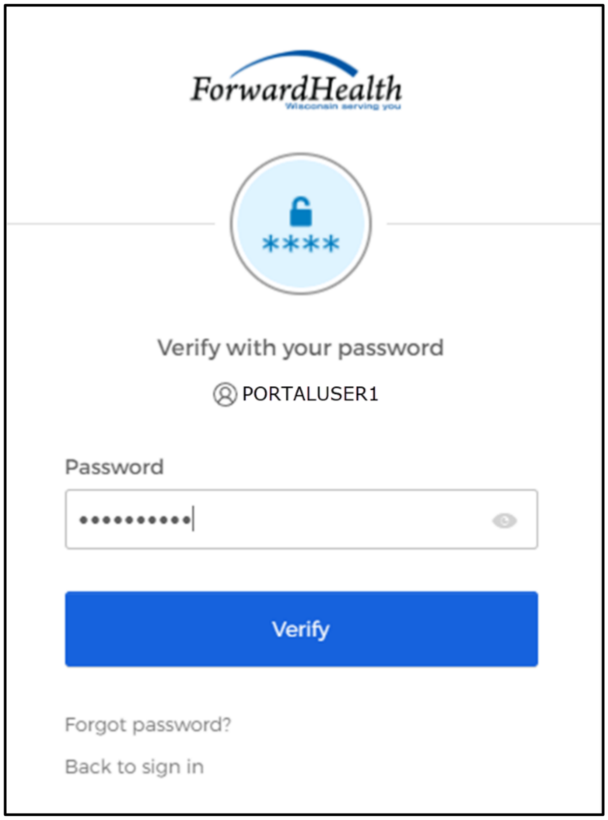


Figure 74 Verify With Your Password Box

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.

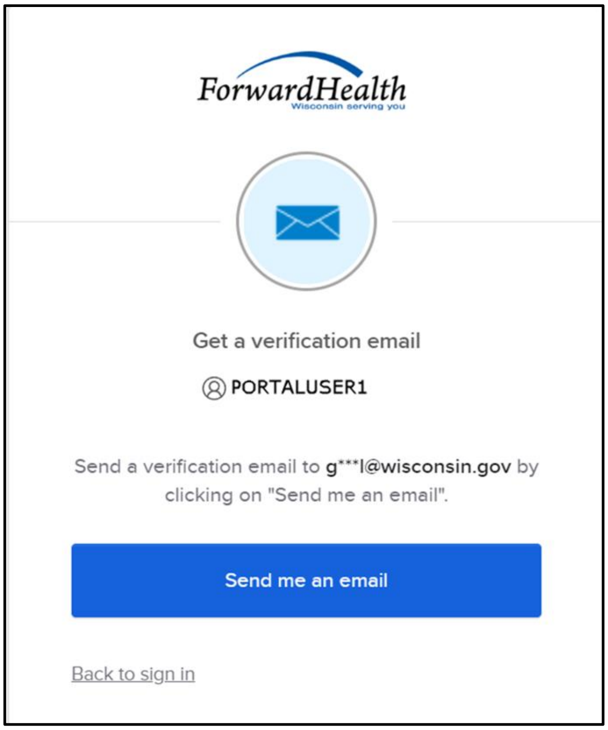


Figure 75 Get a Verification Email Box

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.

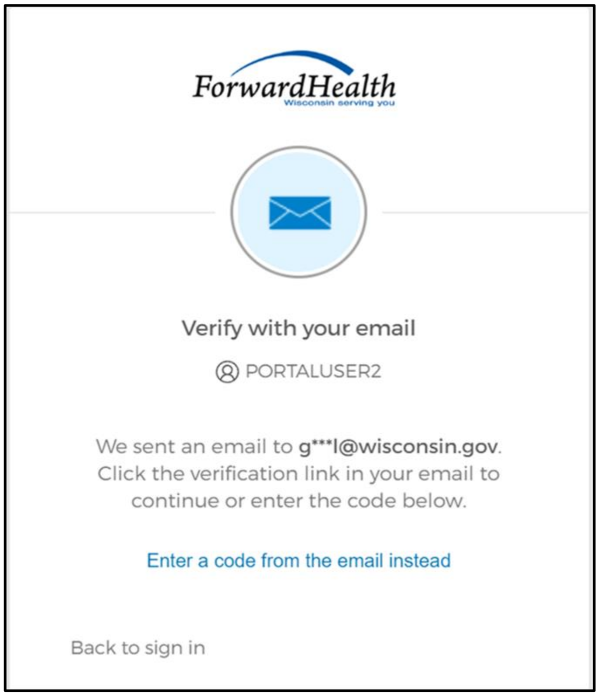


Figure 76 Verify With Your Email Box

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

Figure 77 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.**

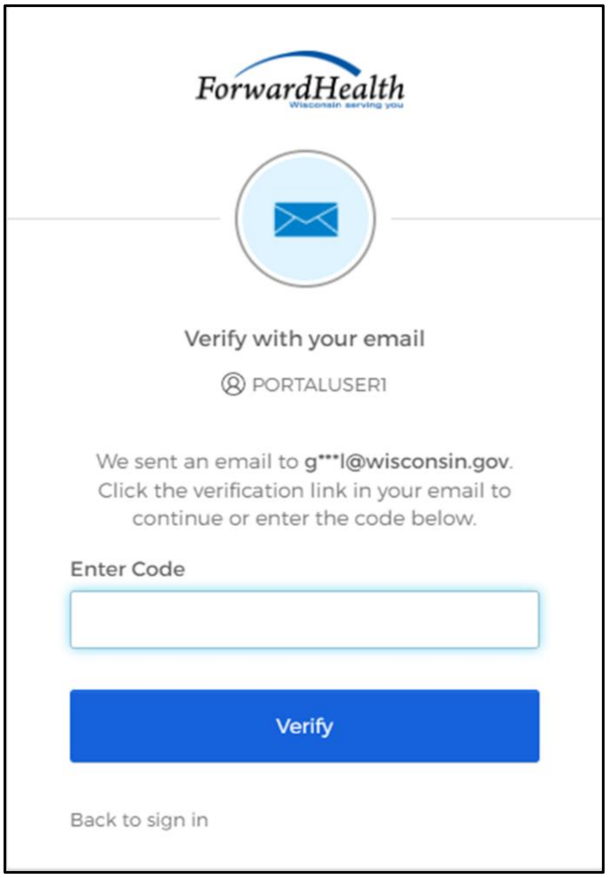


Figure 78 Verify With Your Email Box

A Set up security methods box will be displayed.

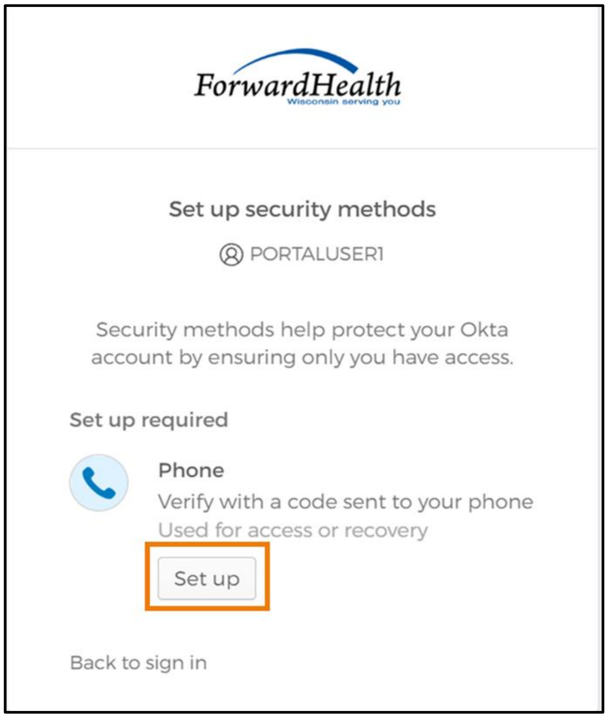


Figure 79 Set Up Security Methods Box

10. Click **Set up**.

A Set up phone authentication box will be displayed.

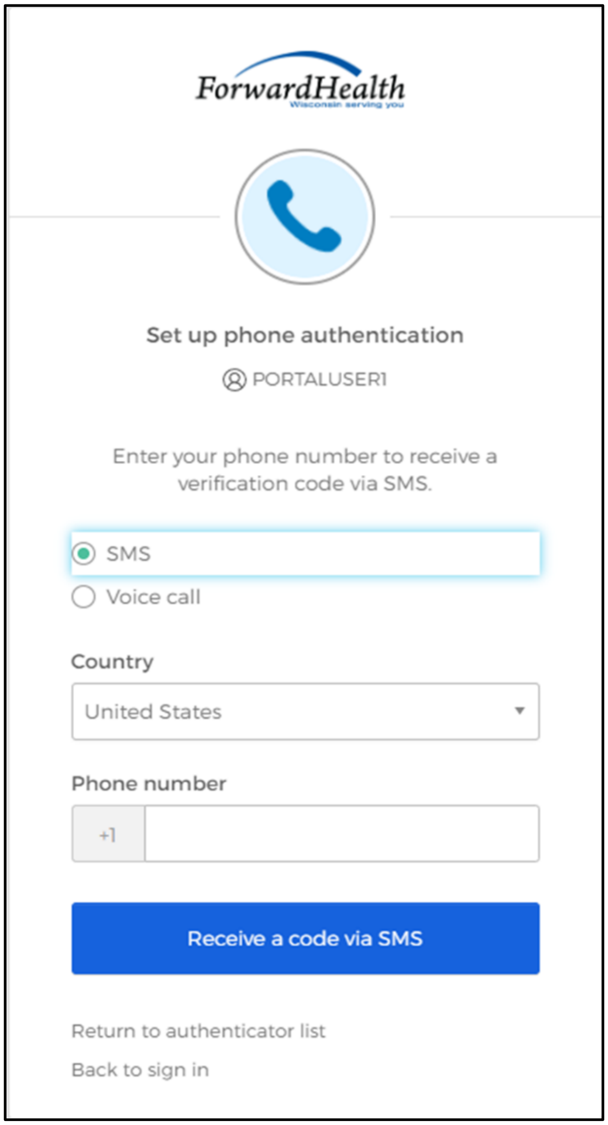


Figure 80 Set Up Phone Authentication Box

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.

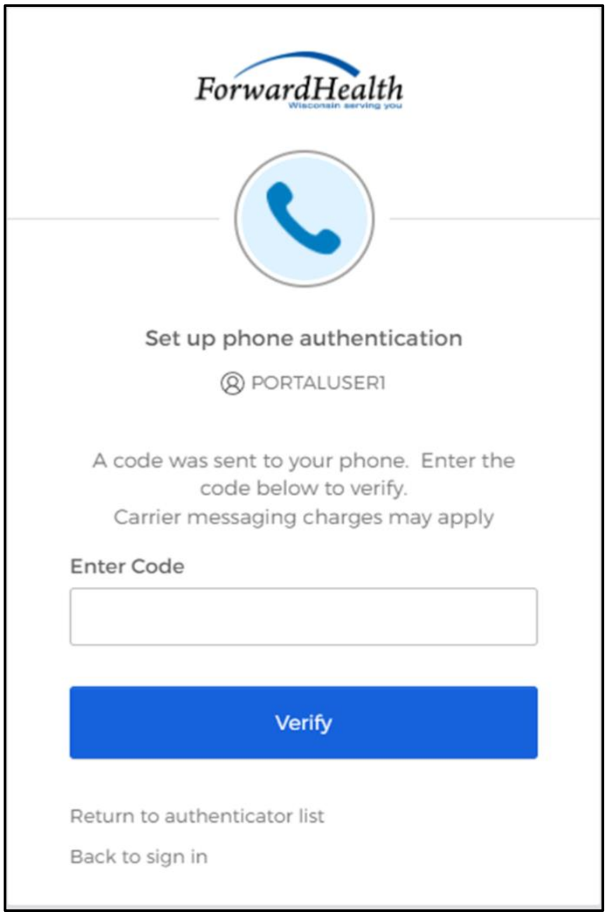


Figure 81 Set Up Phone Authentication Box

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.

6 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.

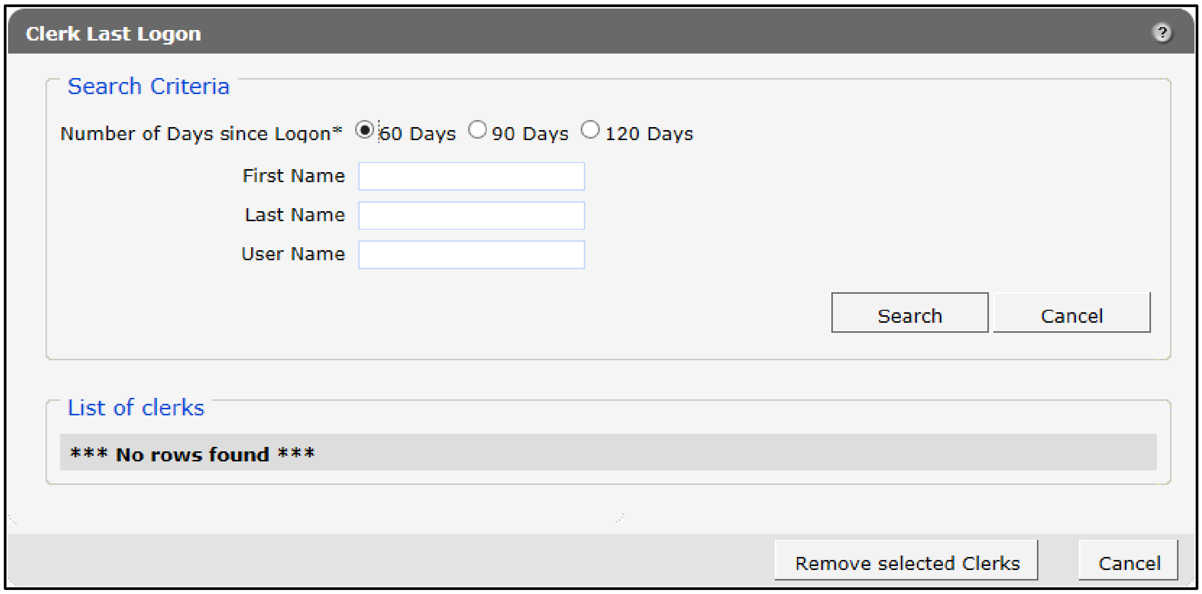


Figure 82 Clerk Maintenance Search Panel

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.

6.1 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.

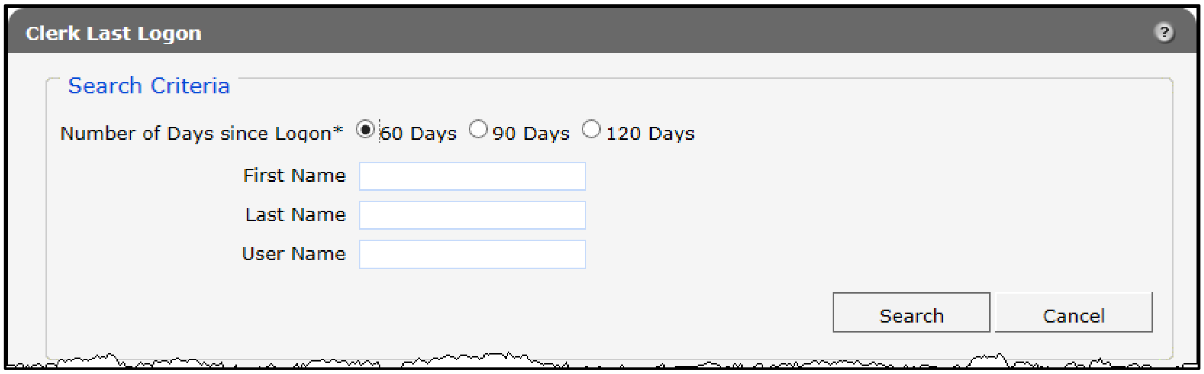


Figure 83 Search Criteria Section

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

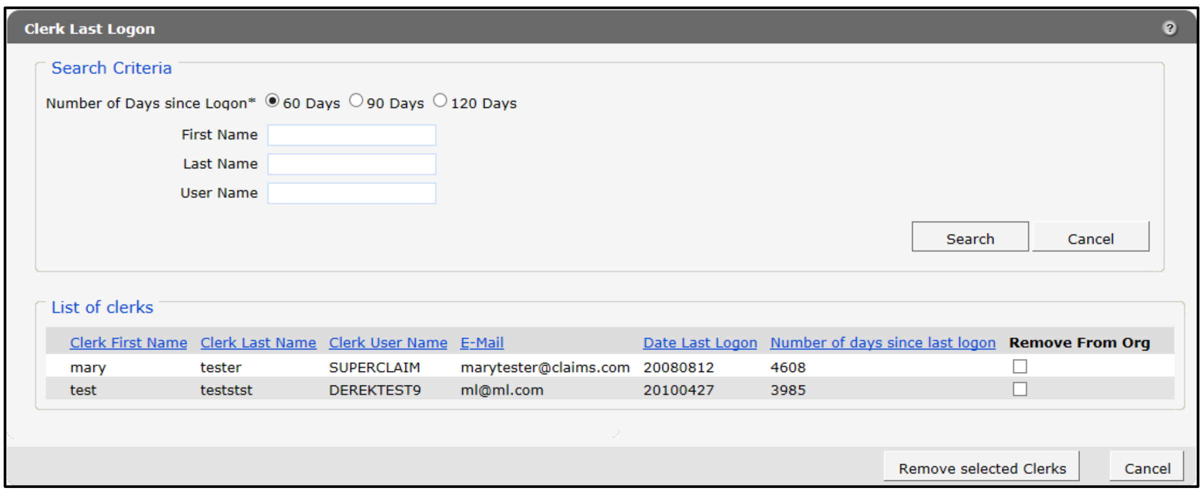


Figure 84 List of Clerks Section

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 Portal account page.

7 Demographic Maintenance Tool

The demographic maintenance tool on the Portal allows EVV providers to securely, efficiently, and conveniently update provider information such as addresses and tax information.

When an EVV provider updates information using the demographic maintenance tool, in most cases, ForwardHealth immediately updates the provider's information, which allows for more efficient business practices.

1. Access the Portal at forwardhealth.wi.gov/.

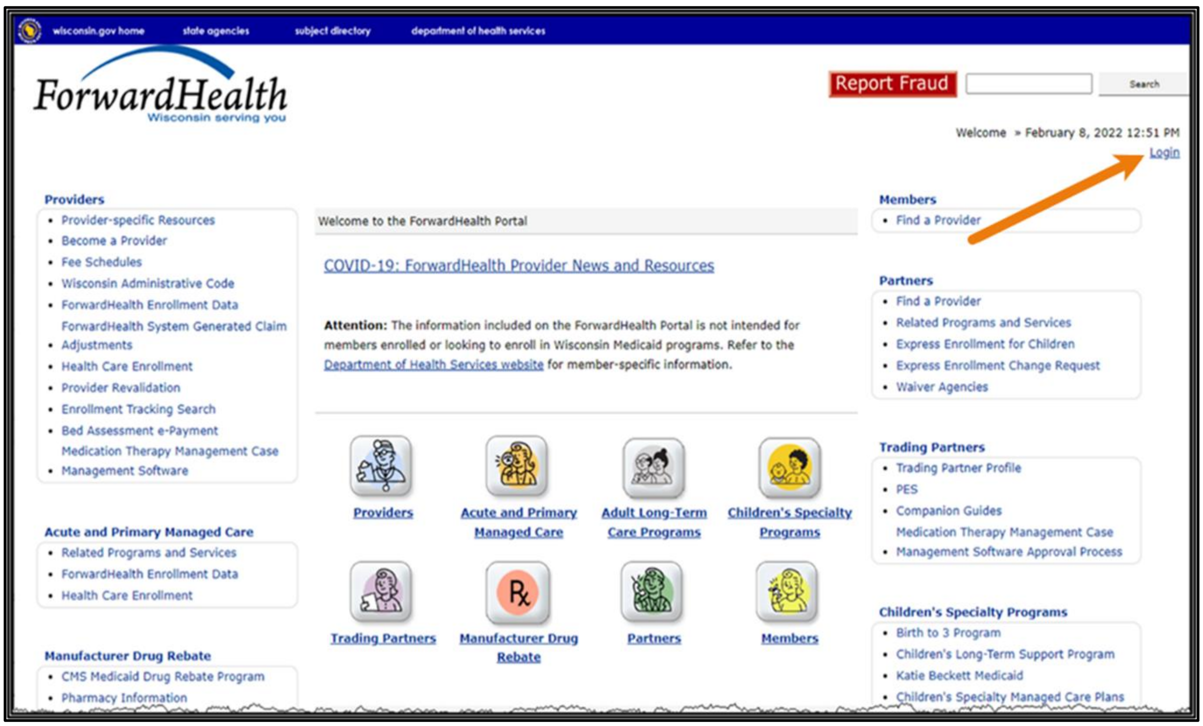


Figure 85 Portal Homepage

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

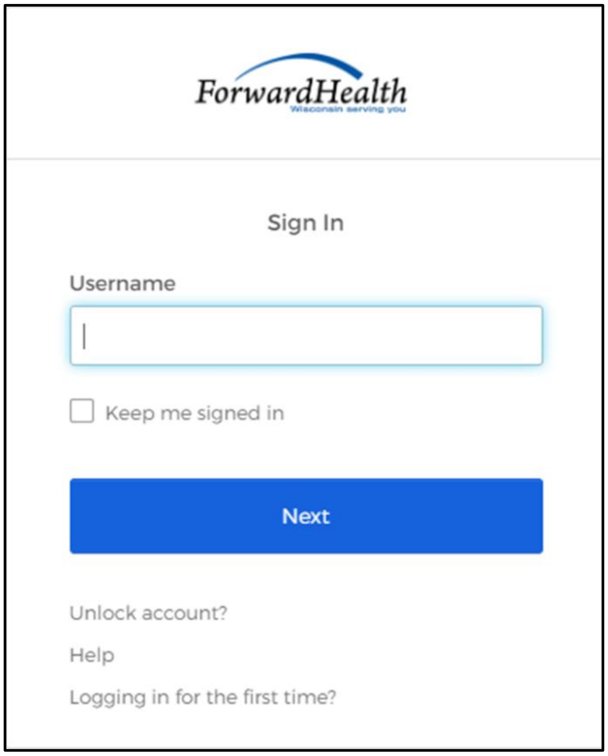


Figure 86 Sign-In Box

3. Enter the user's username.

4. Click **Next**.

A Verify with your password box will be displayed.

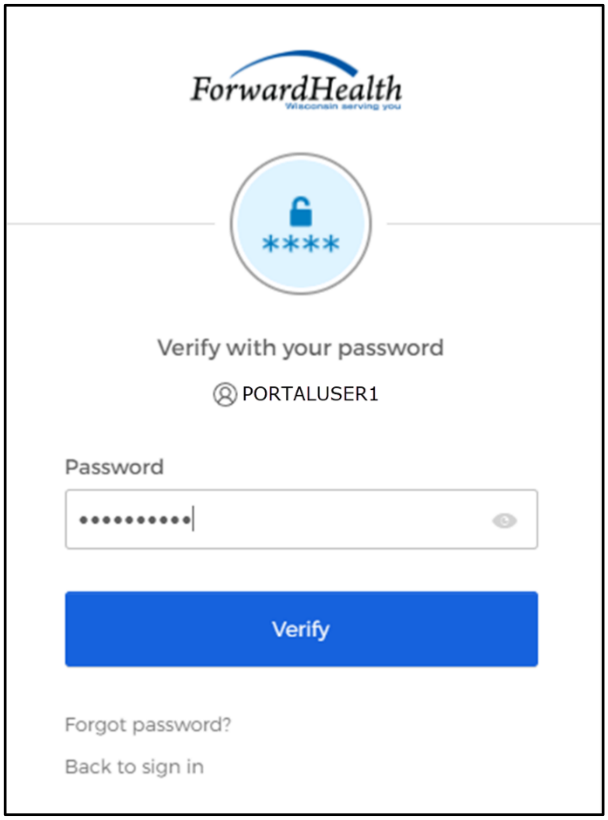


Figure 87 Verify With Your Password Box

5. Enter the user’s password.

6. Click **Verify**. The secure Provider page will be displayed.

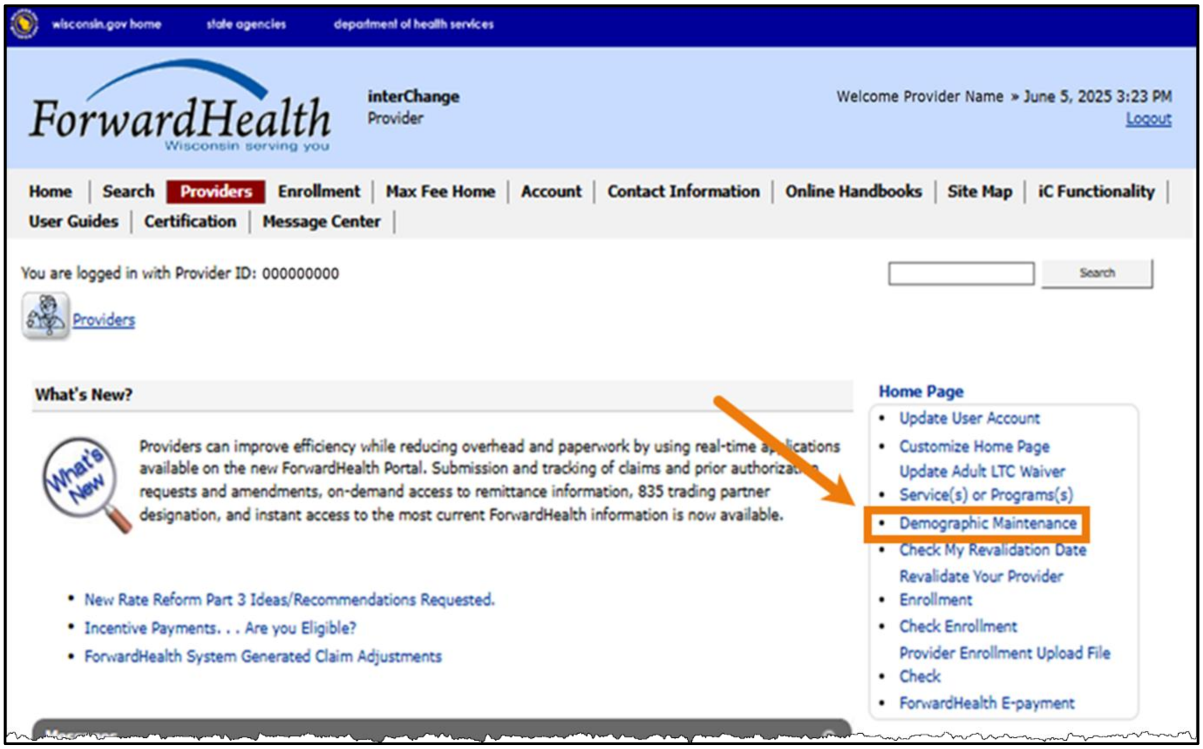


Figure 88 Secure Provider Page

7. Click **Demographic Maintenance** and follow the instructions in the [ForwardHealth Portal Demographic Maintenance Tool User Guide](). This user guide includes a chapter with Adult Long-Term Care Waiver Services panels.

8 Worker Association

For the purposes of EVV, providers are required to add, or associate, each of their workers who provide personal care, applicable supportive home care, or home health care services for Medicaid members. Providers can use the Portal by using the Add Worker or Upload Worker File links under the Electronic Visit Verification Links section of their secure Provider page of the Portal. Providers may also indicate if a worker is exempt from EVV requirements if the worker is not required to capture EVV for any of the people they provide services to for the agency. A list of EVV service codes that require EVV in Wisconsin is available on the DHS website. Providers can access the links under the Home Page, Quick Links, and Electronic Visit Verification sections.

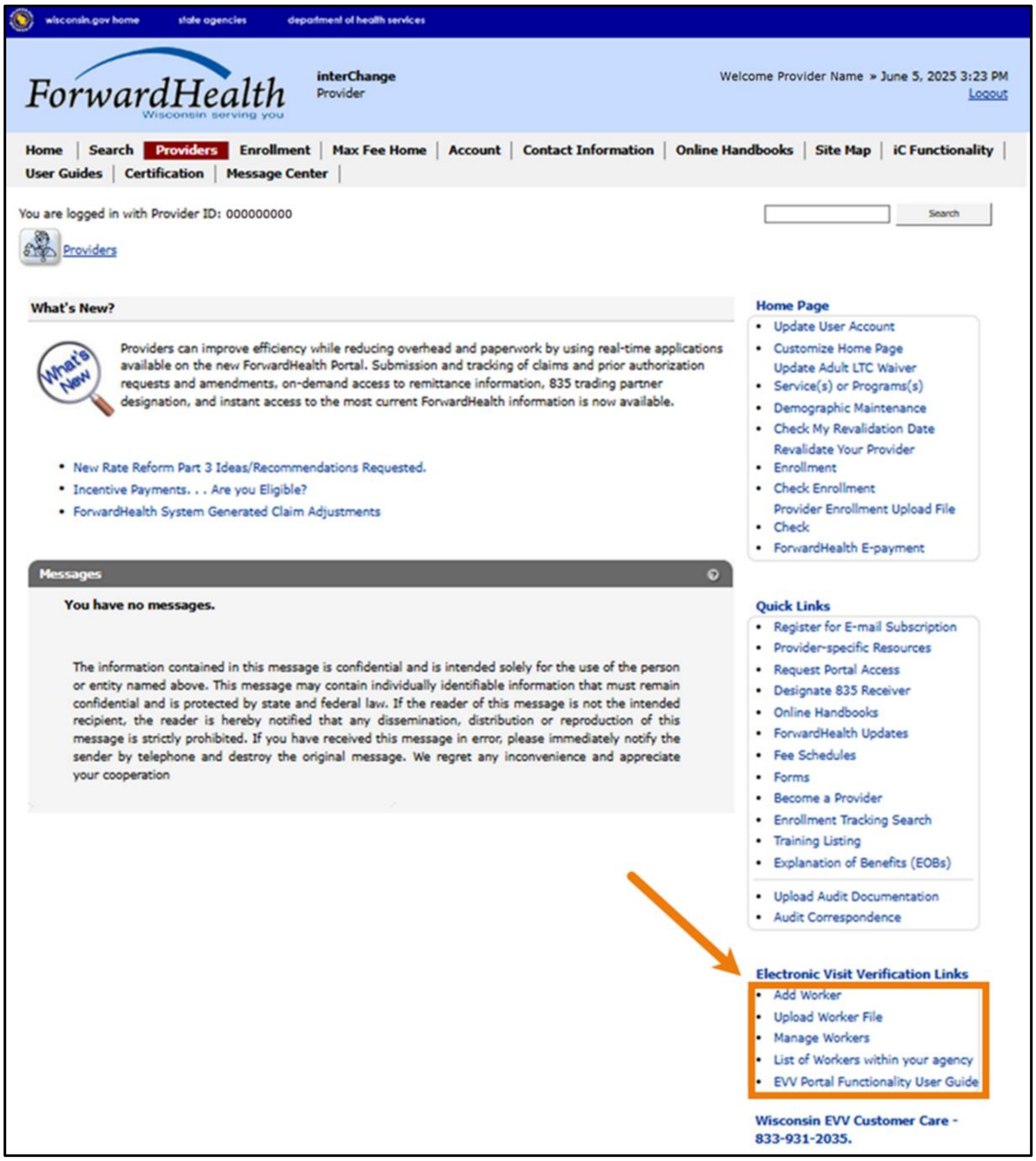


Figure 89 Secure Provider Page—Electronic Visit Verification Links

8.1 Add Worker

This method of worker association allows a provider to manually enter an individual worker's information. To avoid duplication, always start by searching for the worker first.

1. Click **Add Worker** under the Electronic Visit Verification Links section of the secure Provider page. The Add Worker panel will be displayed.

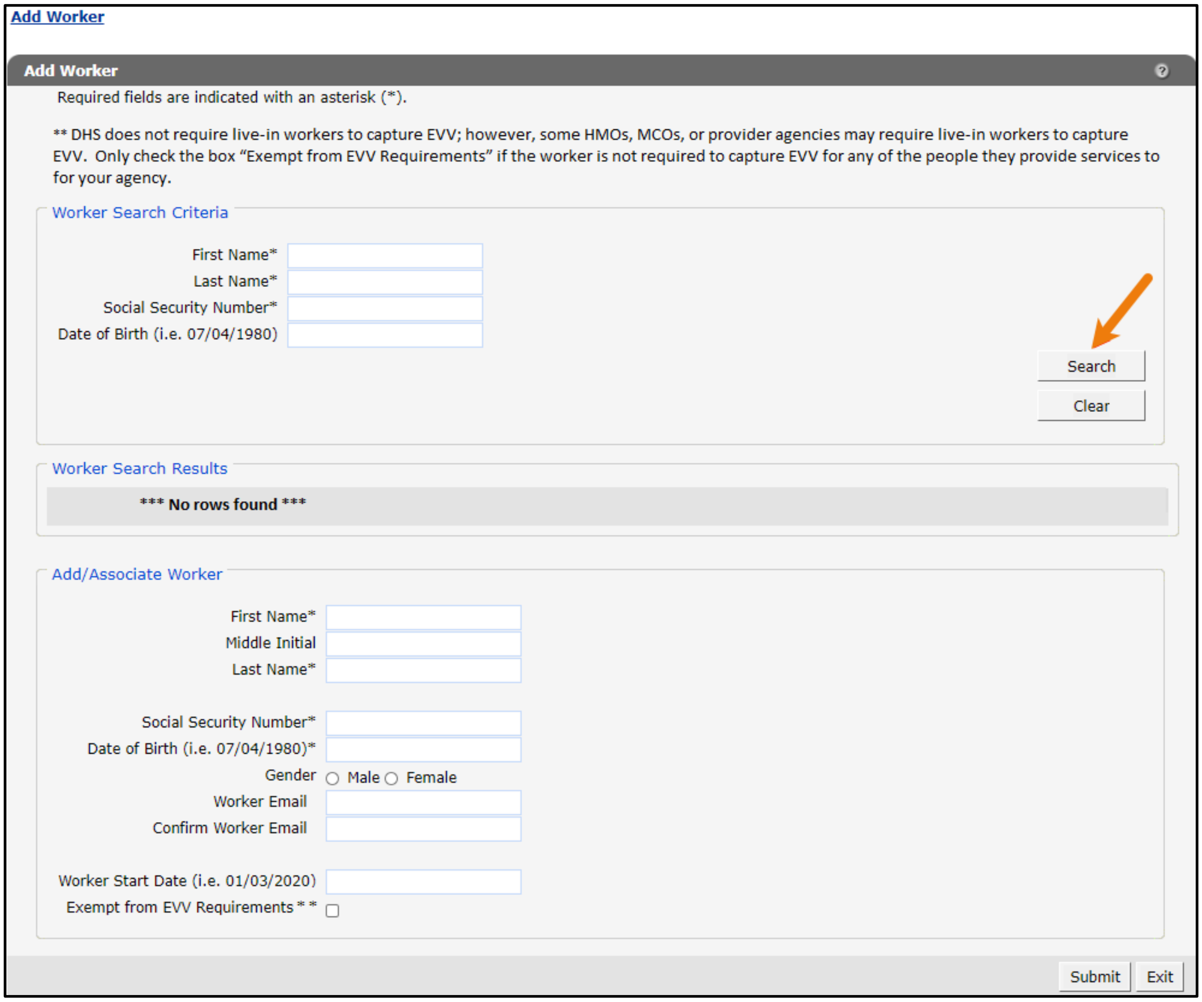


Figure 90 Add Worker Panel

2. Enter the worker's first name, last name, Social Security number, and date of birth into the fields in the "Worker Search Criteria" section. The last name and Social Security number fields are required to perform a worker search.

3. Click **Search**. The panel will refresh and display any results in the "Worker Search Results" section. If no matches to the worker's information are found in the system, a "No Match Found" message will be displayed under Worker Search Results.

8.1.1 No Matches Found

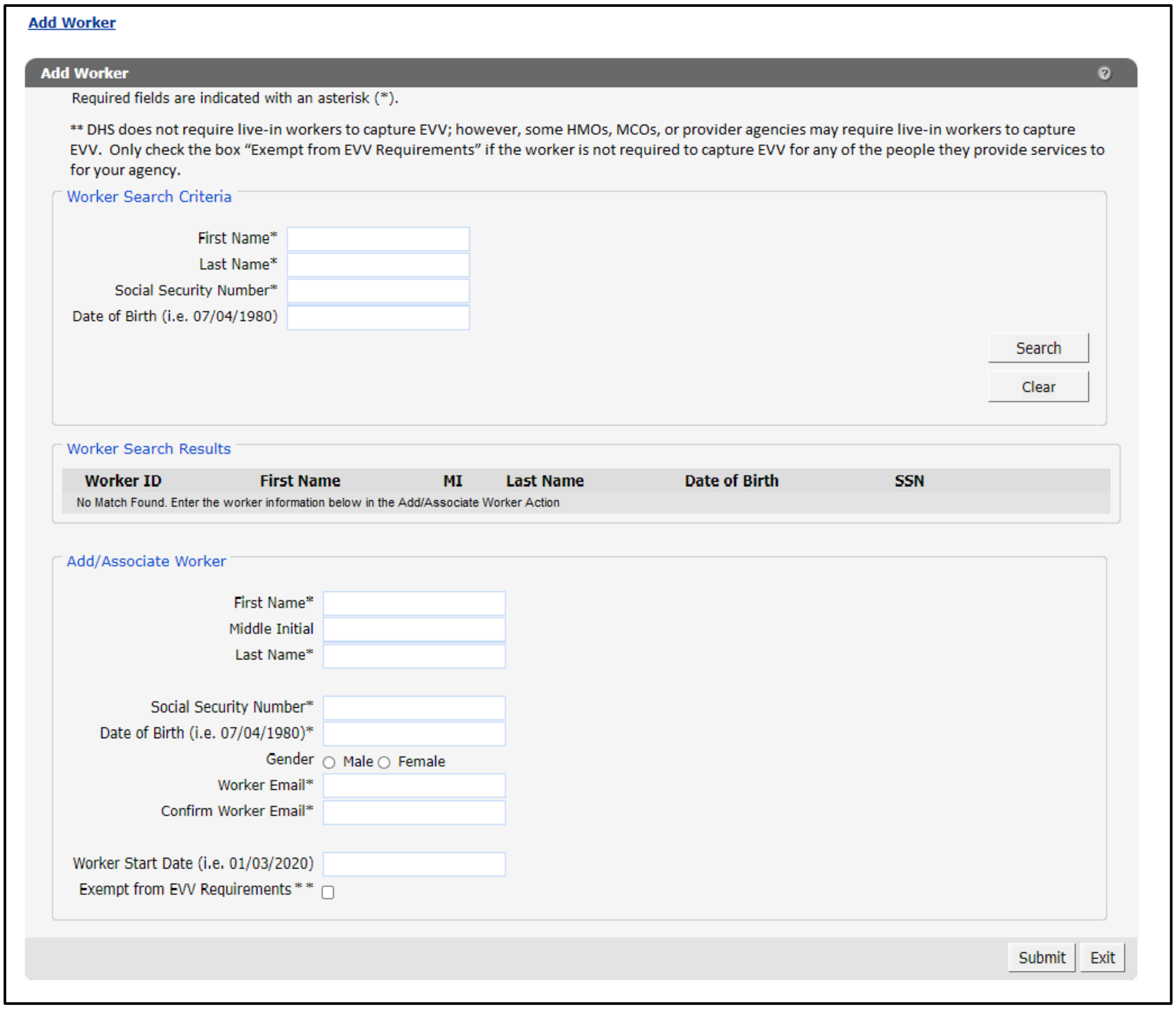


Figure 91 Add Worker Panel With "Worker Search Results" Section

If no match is found, the worker is new to the Portal and will need to be added. Enter the worker's information into the following fields in the "Add/Associate Worker" section:

- First Name
- Middle Initial
- Last Name
- Social Security Number
- Date of Birth (in MM/DD/YYYY format)
- Gender (optional)

- Worker Email—The email address must be unique to that worker and cannot be used by anyone else. The worker email can be used for multiple providers if the worker chooses to do so.

- Confirm Worker Email

- Worker Start Date (in MM/DD/YYYY format)—The worker's EVV start date is the first date the worker will begin or began using EVV and can be a date of up to 365 days in the past, today's date, or a future date. If the worker's EVV start date field is left blank, the system will default the EVV start date to today's date. The worker's EVV start date indicates the date the worker is associated with the provider for the purposes of EVV and their information sent to Sandata. The worker will receive an email with a temporary password for the option to access Sandata Mobile Connect (SMC) one or two days after they have been entered in the Portal.

- Exempt from EVV Requirements**—This box should be checked if the provider determines that a worker is exempt from EVV requirements. The system will assign the worker a unique ID; however, the worker's information will not be sent to Sandata on the worker file.

  If the provider determines a worker who was previously exempt from EVV requirements is no longer exempt, the provider can use the Manage Workers panel to uncheck the box in the Exempt from EVV Requirements** field.

  If the box is checked, the Worker Email and Confirm Worker Email fields are optional. If the provider enters a worker email in the Worker Email field, the Confirm Worker Email field is required. If the box is not checked, the Worker Email and Confirm Worker Email fields are required.

4. Click **Submit**. The Worker Submitted panel will be displayed.

Figure 92 Worker Submitted Panel

The Worker Submitted panel confirms that the worker has been correctly associated with the user's provider and displays the worker's unique ID number for Sandata EVV purposes. This number will also be the worker's Santrax ID if using the DHS-provided EVV solution. Provide this number to the worker if using the DHS-provided EVV solution (Sandata).

5. Click **Save** to save a copy of the corresponding file. The user does not need to click **Save** to view the report and finish associating the worker.

6. Click **Exit** to return to secure Provider page.

8.1.2 Match Found

When a user searches for a worker and a match is found within the system, their information will be displayed in the "Worker Search Results" section. Information must be checked to ensure it is accurate. Workers will only be assigned one worker ID on the Portal throughout their career so, if the worker worked for an agency in the recent past or is currently doing so, this number will remain the same.

1. Click the row containing the worker's name. The panel will be refreshed, and the worker's information will be populated in the fields under the "Add/Associate Worker" section.

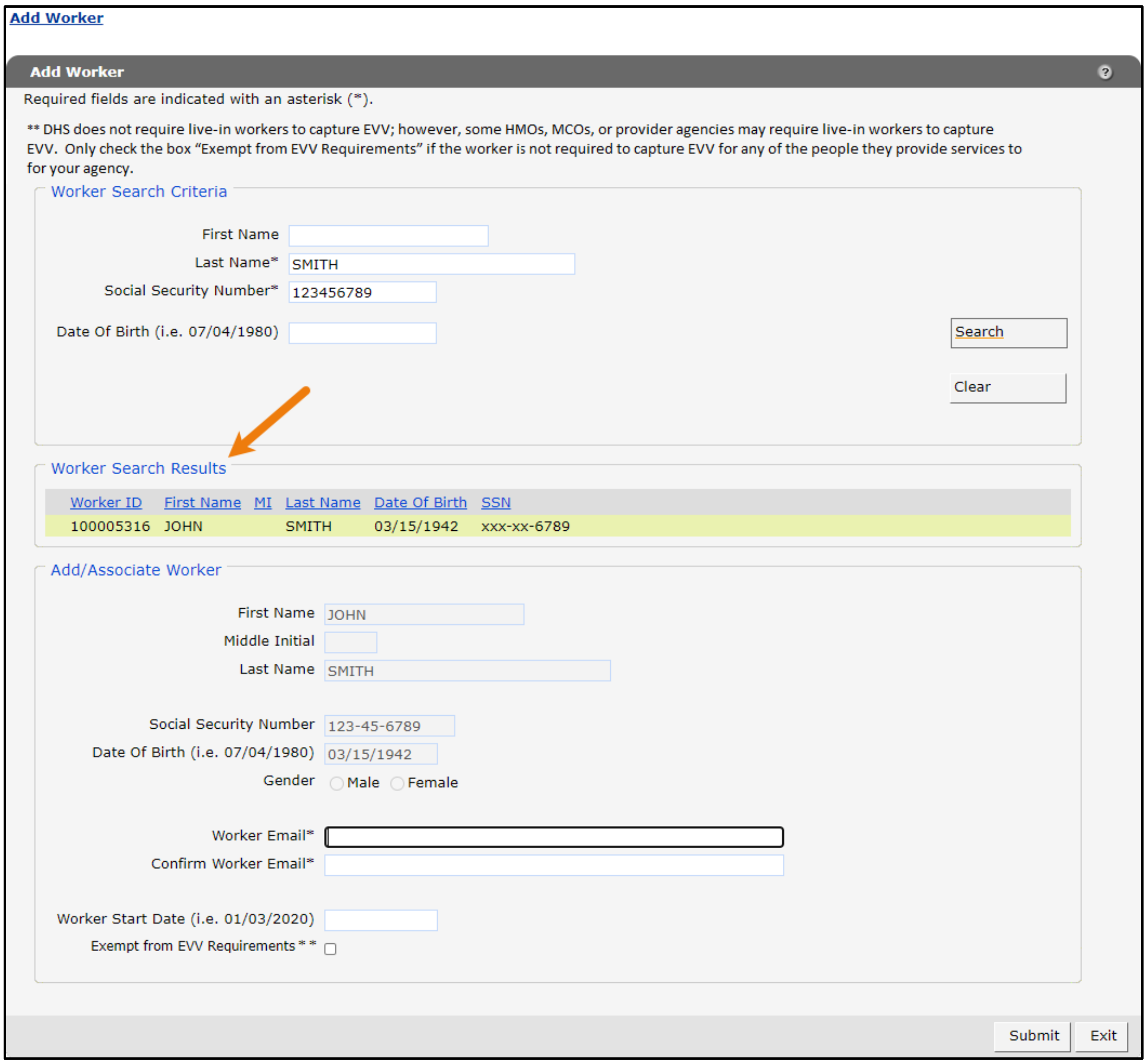


Figure 93 Add Worker Panel With Worker Information Populated

2. Enter the worker's email address in the Worker Email and Confirm Worker Email fields. The email address must be unique to that worker and cannot be used by anyone else. The worker's email can be used for multiple providers if the worker chooses to do so.

   Note: If the box is checked in the Exempt from EVV Requirements** field, the Worker Email and Confirm Worker Email fields are optional.

3. Enter the first date the worker will begin or began using EVV in the Worker Start Date field in MM/DD/YYYY format.

   Note: The worker's EVV start date is the first date the worker will begin or began using EVV and can be a date of up to 365 days in the past, today's date, or a future date. If the worker's EVV start date field is left blank, the system will default the EVV start date to today's date. The worker's EVV start date indicates the date the worker is associated with the provider for the purposes of EVV and their information sent to Sandata. The worker will receive an email with a temporary password for the option to access SMC one or two days after they have been entered in the Portal.

4. Click **Submit**. The Worker Submitted panel will be displayed.

Figure 94 Worker Submitted Panel

   The Worker Submitted panel confirms that the worker has been correctly associated with the provider and displays the worker's unique ID number for Sandata EVV purposes. This number will also be the worker's Santrax ID if using the DHS-provided EVV solution. Provide this number to the worker if using the DHS-provided EVV solution (Sandata).

5. Click **Save** to save a copy of the corresponding file. The user does not need to click **Save** to view the report and finish associating the worker.

6. Click **Exit** to return to the secure Provider page.

8.2 Upload Worker File

The Upload Worker File method of worker association allows users to associate multiple workers at once by uploading a prepared Microsoft Excel file.

1. Click **Upload Worker File** under the Electronic Visit Verification Links menu of the secure Provider page. The Upload Worker File panel will be displayed.

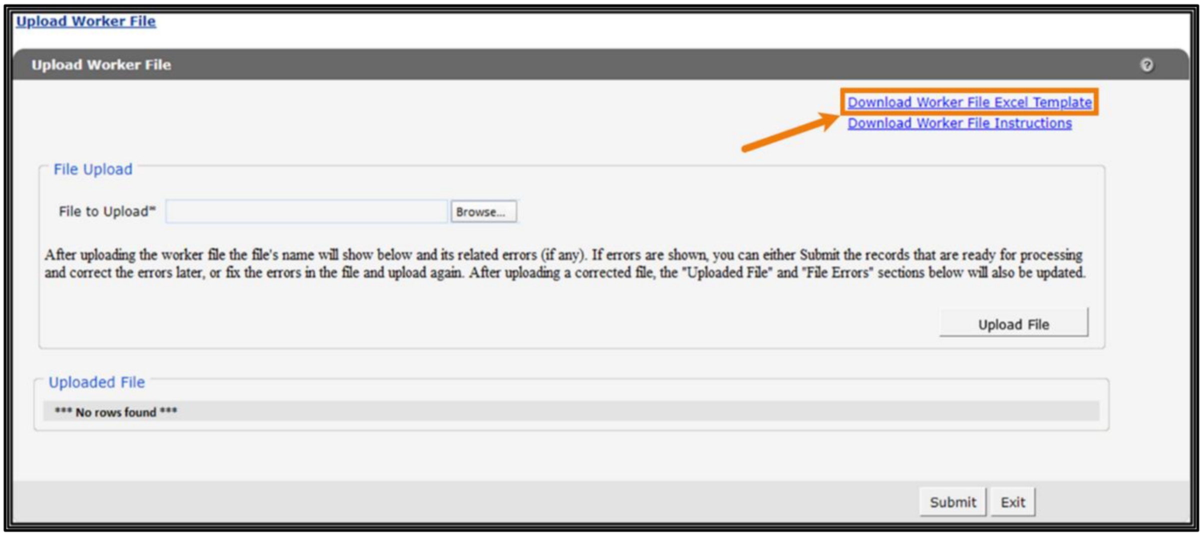


Figure 95 Upload Worker File Panel

2. Click **Download Worker File Excel Template** and save the template to the user's computer.

3. Navigate to the saved location on the user's computer and open the template file.

4. Within the template file, enter the information for the workers that will be associated to the provider. List the worker's first name followed by the last name as indicated in the template file.

   Note: The email address must be unique to that worker and cannot be used by anyone else. The worker's email can be used for multiple providers if the worker chooses to do so. The worker's EVV start date is the first date the worker will begin or began using EVV and can be a date of up to 365 days in the past, today's date, or a future date. If the worker's EVV start date field is left blank, the system will default the EVV start date to today's date. The worker's EVV start date indicates the date the worker is associated with the provider for the purposes of EVV and their information sent to Sandata. The worker will receive an email with a temporary password for the option to access SMC one or two days after they are entered in the Portal.

   Valid values for the Exempt_from_EVV_Requirements column are "Y" for yes, "N" for no, or blank. If the column is blank, the default will be "N." If an invalid value is entered, the following message will be displayed: "The Exempt from EVV Requirements field contains an invalid value." The worker's email address is optional for exempt workers.

   Fields in bold are required.

	A	B	C	D	E	F	G	H	I	J
1	First_Name	Middle_Initial	Last_Name	SSN	Date_of_Birth	Gender	Worker_Email	Confirm_Worker_Email	Worker_Start_Date	Exempt_from_EVV_Requirements
2	John		Smith	123456789	3/15/1942					Y
3	Sam		Sample	222222222	2/14/1968		sample@gmail.com	sample@gmail.com	6/16/2020	N

Figure 96 Download Worker File Excel Template

5. Once the information is entered, the user should save the file to their computer and exit the Excel application.

6. Return to the Upload Worker File panel.

7. Click **Browse.**

Figure 97 Upload Worker File Panel

8. Locate and select the saved file on the user's computer. Click **Open** to attach the file to the panel.

9. Click **Upload File** to upload the file.

Figure 98 Upload Worker File Panel

10. Once uploading is complete, the panel will be refreshed, and the name of the file and associated results will be displayed in the “Uploaded File” and “File Errors” sections.

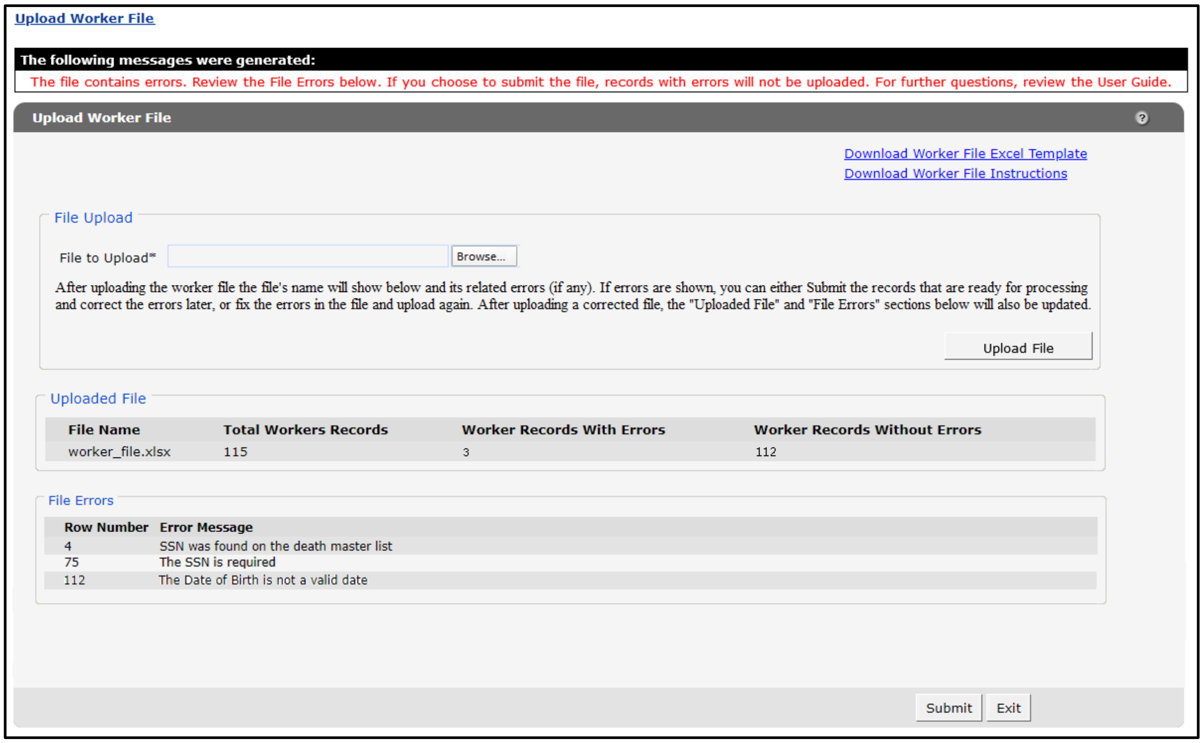


Figure 99 Upload Worker File Panel With Uploaded File Information

If the file contains any errors, they will be displayed and detailed in the “File Errors” section. There are two options if the file contains errors:

- The first option is to correct the errors in the file immediately and re-upload it.

  Note: When the updated file is uploaded, the updated file’s results will replace the previous file’s results.

- The second option is to click **Submit** to upload the file as is to the system.

  Note: Only those worker records without errors will be processed. If this option is chosen, the user will need to restart the process of uploading the file with corrected worker records. A copy of the worker errors can be saved after submission using the options on the next screen.

11. Once the user clicks **Submit** and the workers are associated to the user's provider, the Workers Submitted panel will be displayed.

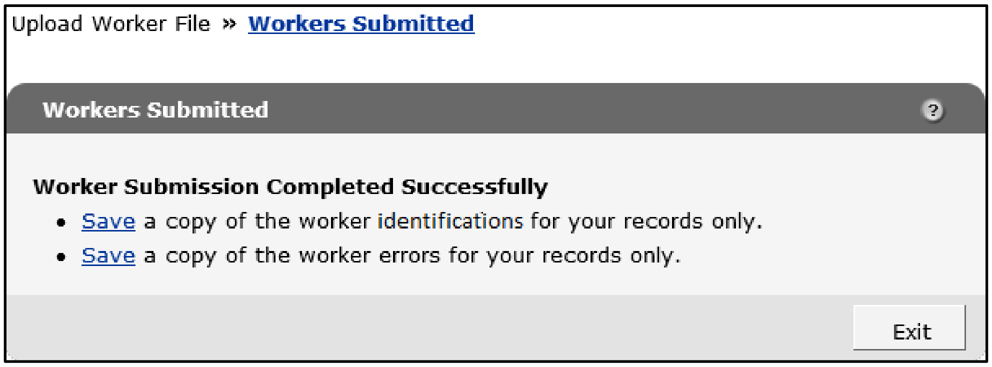


Figure 100 Workers Submitted Panel

12. The Workers Submitted panel allows users to save copies of the worker records that were created within the ForwardHealth system. This information includes their unique worker ID and any copies of the error report for the submitted Excel worker file. Provide this number to the worker if using the DHS-provided EVV solution (Sandata). Click **Save** to save a copy of the corresponding file.

13. Click **Exit** to return to the secure Provider page.

9 Manage Workers

Providers can manage their workers' email addresses and associate them to the providers on the Portal using the Manage Workers tool.

1. Click **Manage Workers** under the Electronic Visit Verification Links section of the secure Provider page. The Manage Workers panel will be displayed.

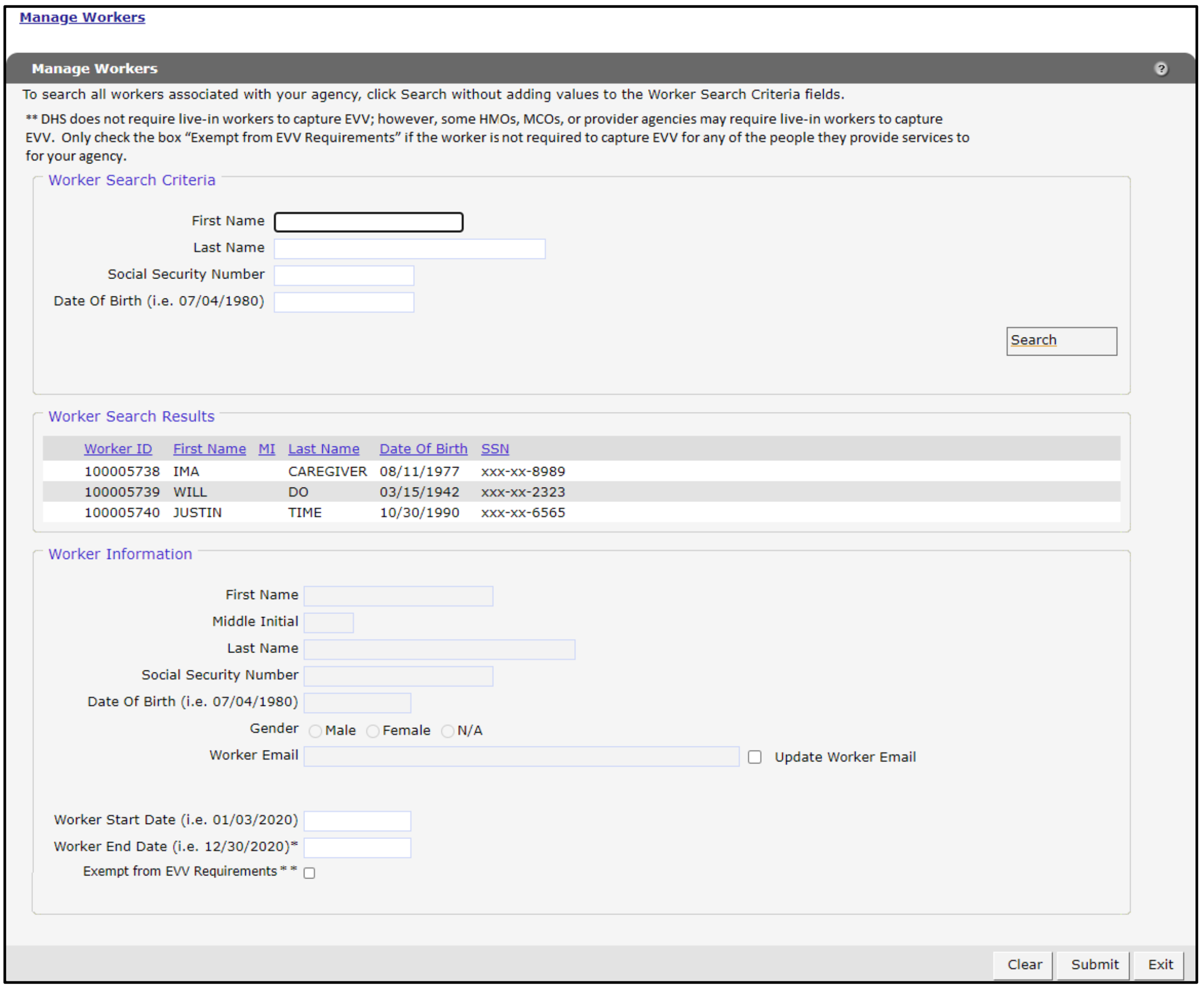


Figure 101 Manage Workers Panel

2. Enter information for the worker whose information needs updating, then click **Search**. The panel will be refreshed and results matching the search criteria will be displayed in the "Worker Search Results" section. The last name and Social Security number fields are required to perform a worker search. If no search criteria were entered and the user selects the Search button, a list of all workers associated with the provider will be displayed.

3. Click the row containing the worker's name. The panel will be refreshed, and the worker's information will be populated in the fields in the "Worker Information" section.

Notes:

- If the box in the Exempt from EVV Requirements** field is checked and a provider determines the worker is no longer exempt from EVV requirements, they can uncheck the box. The provider will also need to add a worker email address. The action of unchecking the box and adding the worker email address will ensure the worker will be sent to Sandata on the worker file.

- The only editable fields are the Worker Email, Worker Start Date, Worker End Date, and Exempt from EVV Requirements**. The employee start date can be backdated up to 365 days in the Worker Start Date field. If changes to other fields are needed, the provider will need to contact Wisconsin EVV Customer Care at 833-931-2035, Monday–Friday, 7 a.m.–6 p.m.

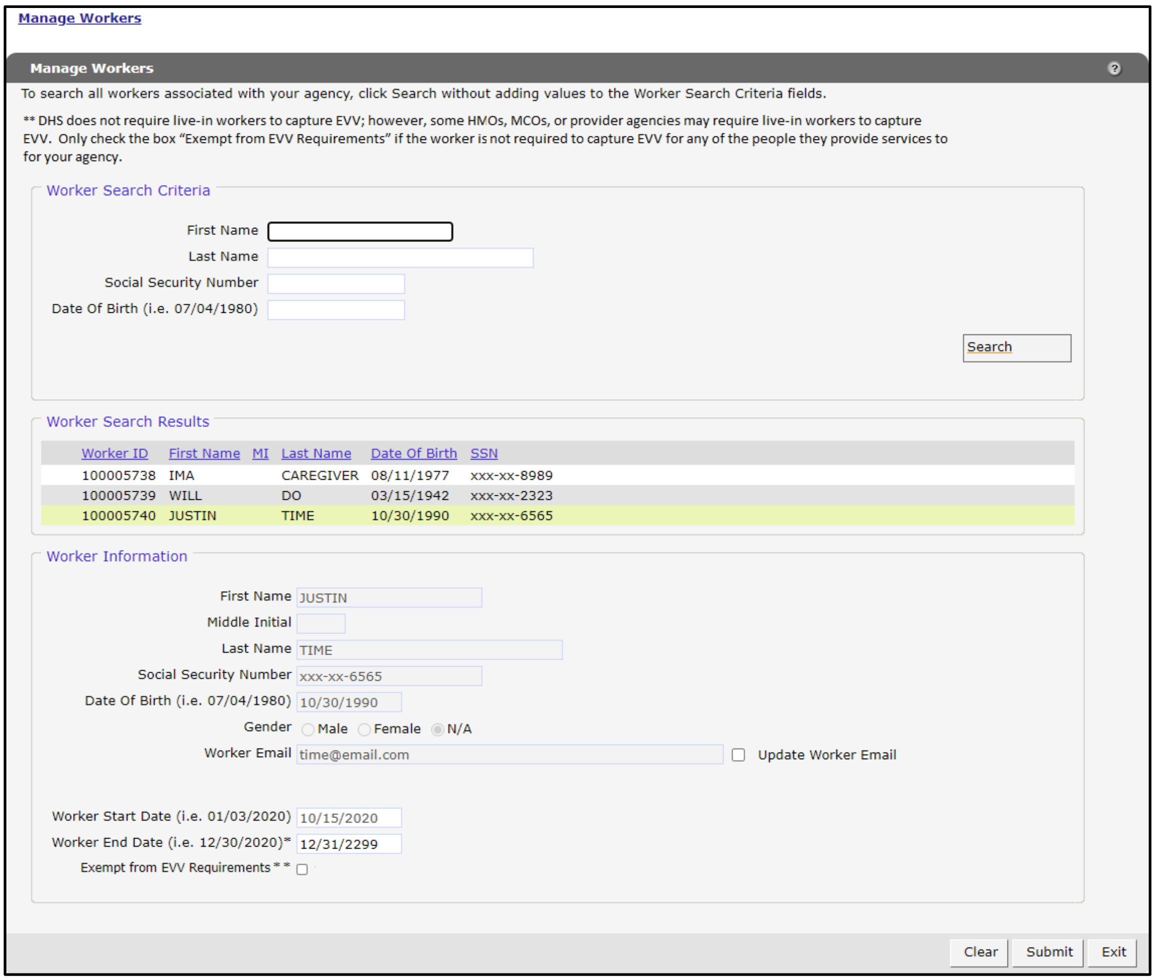


Figure 102 Manage Workers Panel With Worker Information Populated

4. Click the **Update Worker Email** checkbox. The New Worker Email and Confirm New Worker Email fields will be displayed.

Figure 103 New Worker Email Fields

5. Enter the new email for the worker in the fields.

   Note: The email address must be unique to that worker and cannot be used by anyone else. The worker email can be used for multiple providers if the worker chooses to do so.

6. If the worker is no longer employed with the provider, the user can disassociate them from the provider by entering the last date of employment in the Worker End Date field in MM/DD/YYYY format.

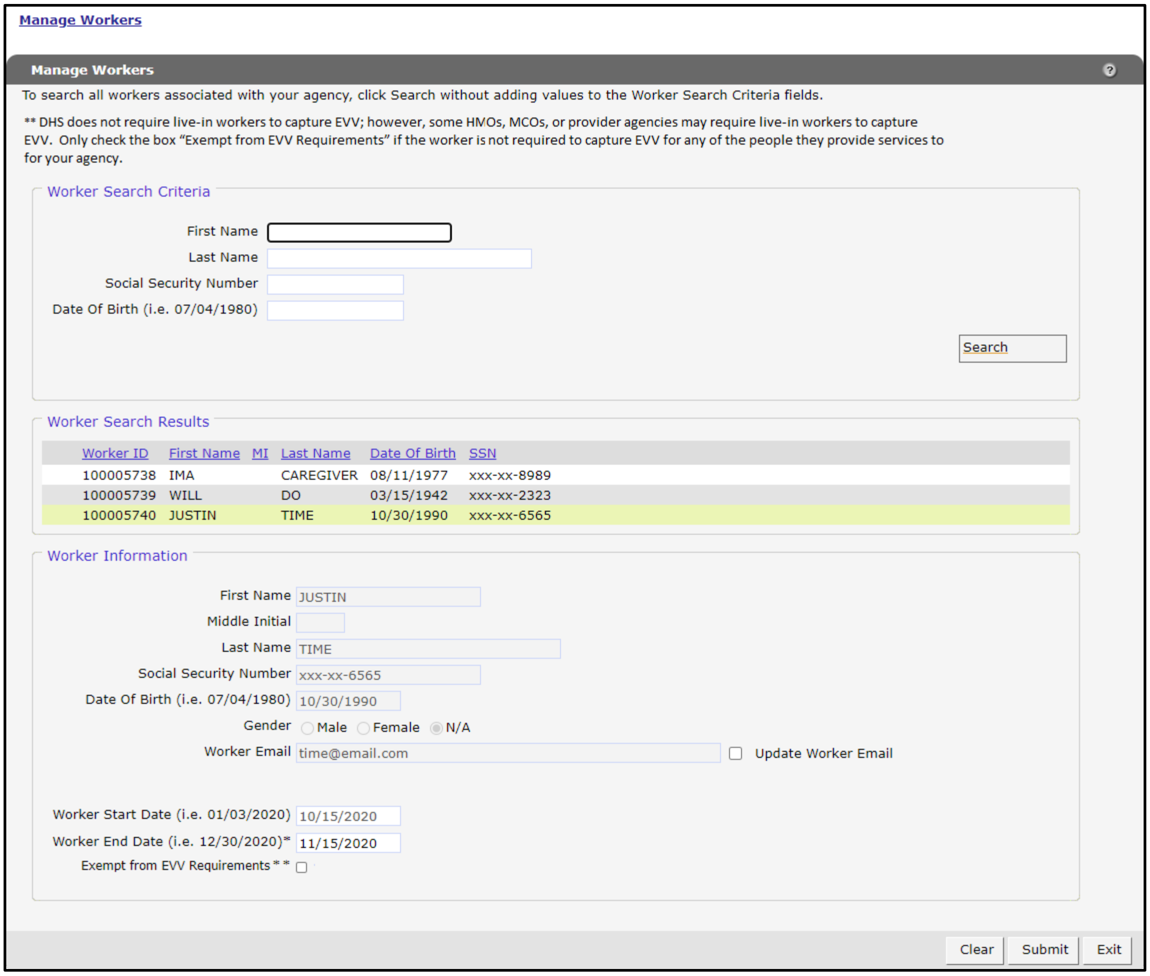


Figure 104 Manage Workers Panel With Disassociating Information

Note: Adding a worker's end date will only affect that provider and does not affect other providers that the worker may be employed with.

7. Click **Submit**. The worker's information will be updated within the ForwardHealth system, and the Worker Change Submitted panel will be displayed.

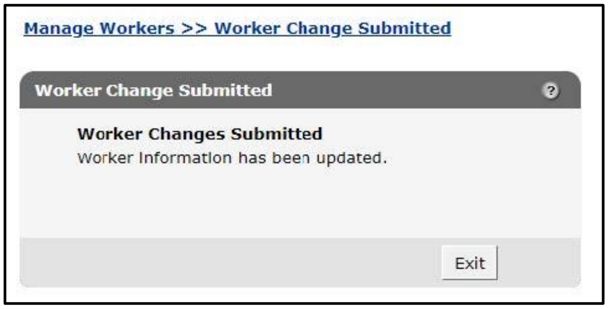


Figure 105 Worker Change Submitted Panel

8. Click **Exit** to return to the secure Provider page.

10 List of Workers Within Your Agency

Users can view reports that list all the workers currently associated with the provider or all workers including workers that have been end-dated.

1. Click **List of Workers within your Agency** under the Electronic Visit Verification Links section of the secure Portal page. The List of Workers panel will be displayed.

Figure 106 List of Workers Within Your Agency Panel

2. Select “All Workers” or “All Active Workers.”

3. Click the Generate Workers Report link and the corresponding file in comma-separated value (CSV) format will be opened. This file can also be saved as an Excel file.

   Note: All active workers will show as the high-end system date of 12/31/2299.

	A	B	C	D	E	F	G	H
1	Title: AgencyID 100000001 EVV IDENTIFICATION UAT - All Workers							
2	Worker ID	First Name	Last Name	SSN	Worker Email	Start Date	End Date	Exempt from EVV Requirements
3	100005309	JUSTIN	TIME	xxx-xx-2920	time@email.com	7/22/2020	7/30/2020	N
4	100005310	WILL	DO	xxx-xx-6271		7/22/2020	12/31/2299	Y
5	100005323	IMA	CAREGIVER	xxx-xx-6756	caregiver@email.com	7/27/2020	12/31/2299	N

Figure 107 List of All Workers

	A	B	C	D	E	F	G	H
1	Title: AgencyID 100000001 EVV IDENTIFICATION UAT - All Active Workers							
2	Worker ID	First Name	Last Name	SSN	Worker Email	Start Date	End Date	Exempt from EVV Requirements
3	100005310	WILL	DO	xxx-xx-6271		7/22/2020	12/31/2299	Y
4	100005323	IMA	CAREGIVER	xxx-xx-6756	caregiver@email.com	7/27/2020	12/31/2299	N

Figure 108 List of All Active Workers