WPS GHA Portal User Manual

Wisconsin Physicians Service Insurance Corporation

http://www.wpsgha.com

TABLE OF CONTENTS

WPS GHA Portal Overview ................................................................................................................................. 4

User Responsibilities, Access, and Management

User Responsibilities (All Users)
Reporting a Security Incident ............................................................................................................................. 5
Sharing WPS GHA Portal User Login IDs ............................................................................................................ 5

Access to WPS GHA Portal
Register as a WPS GHA Portal Administrator for a Medicare Provider .............................................................. 5
Request Access through Your NPI Administrator ................................................................................................ 10
Requesting Access for Additional Administrators (more than two) .................................................................. 12
Logging In ............................................................................................................................................................ 12
Multi-Factor Authentication ................................................................................................................................ 13
Logout .................................................................................................................................................................... 22
Recertification ..................................................................................................................................................... 22
Account Reactivation .......................................................................................................................................... 25

Username/Password Management
Initial Password ........................................................................................................................................................ 29
Password Requirements ....................................................................................................................................... 29
Auto Created Password ....................................................................................................................................... 30
Expired Password ............................................................................................................................................... 30
Forgot Username/Password ................................................................................................................................. 30
Locate Administrator to Update Your Account .................................................................................................... 33

My Account Tools

My Dashboard
User Dashboard Windows ..................................................................................................................................... 38
Pending Access Request (Administrators Only) ................................................................................................... 38
Registration Approvals (Administrator Only) ........................................................................................................ 40
Blackout NPIs .................................................................................................................................................... 41
User Search (Administrators Only) ...................................................................................................................... 42
Quick Links ......................................................................................................................................................... 43
New Messages ................................................................................................................................................... 43

My Profile
Change My Password ......................................................................................................................................... 44
Change Security Q&As ....................................................................................................................................... 45
Disable My Account ............................................................................................................................................ 46
My Service Locations ....................................................................................................................................... 46

Message Center
Send a Secure Message ....................................................................................................................................... 48
Check Message Center Status ............................................................................................................................ 54

November 2019
Wisconsin Physicians Service Insurance Corporation

USER ADMINISTRATION (ADMINISTRATORS ONLY)
User Administration ......................................................................................................................................................... 57
Add New User ................................................................................................................................................................. 58
Find and Administer Current Users ................................................................................................................................. 59
Removing Access for Standard and Eligibility Users ...................................................................................................... 60

MY TRANSACTIONS

ELIGIBILITY
Eligibility Check ............................................................................................................................................................... 62
Available Eligibility Information ........................................................................................................................................ 65

MEDICARE BENEFICIARY IDENTIFIER (MBI)
Medicare Beneficiary Identifier (MBI) Lookup ................................................................................................................ 70

CLAIMS (PART B PAPER CLAIMS SUBMITTERS ONLY)
Register for Online Claim Entry ....................................................................................................................................... 71
Submit New Claim ........................................................................................................................................................... 72
Specialty Claim Fields ..................................................................................................................................................... 80

CLAIM INQUIRY
Claim Status – Part A and Part B .................................................................................................................................... 82
Claim Details ................................................................................................................................................................... 84
Claim Actions ................................................................................................................................................................... 88

CLERICAL ERROR REOPENING (CER)
Submitting a Clerical Error Reopening (CER) ................................................................................................................. 89
Common Error Messages and Their Causes .................................................................................................................. 91

OVERPAYMENTS (OCA)
Overpayment Claim Adjustments (OCA). ........................................................................................................................... 92

MEDICAL DOCUMENTATIONS
Search Documentation .................................................................................................................................................... 95
ADR Response .......................................................................................................................................................... 97
ADR Response Using Claim Inquiry ................................................................................................................................... 98
Post-Payment Review Tab .............................................................................................................................................. 101

REMITTANCE ADVICE
Obtain a Full Duplicate from Remittance Search .............................................................................................................. 103
Obtain Remittance from Claim Search ............................................................................................................................ 105

MEDICARE eREFUNDS
Searching for Previous eRefunds .................................................................................................................................... 106
Submitting an Electronic Refund ........................................................................................................................................ 108

LETTER SEARCH (ADR AND DEMAND LETTERS)
Searching for and Responding to an ADR or Demand Letter .............................................................................................. 112

APPEAL SEARCH (REDETERMINATIONS)
Submitting a Part B Redetermination .............................................................................................................................. 116
Appeal Status ........................................................................................................................................................... 120
Portal Submitted Appeals ................................................................................................................................................ 121

November 2019
WPS GHA Portal Overview

WPS GHA Portal Overview
The WPS GHA Portal is a comprehensive and secure alternative to obtain Medicare patient eligibility and claim status. Partnered with the Centers for Medicare & Medicaid Services (CMS), who governs the security regulations and policies of the portal, WPS Government Health Administrators is pleased to be able to provide this convenient and efficient tool to our Medicare providers.

The portal offers many functions detailed below in this user manual. The most frequently accessed functions are eligibility and claim status. The portal uses the CMS HIPAA Eligibility Transaction System (HETS) 270/271 transaction to obtain the most current patient eligibility while the claim status function uses the Claims Processing Shared Systems. In addition, the portal offers the ability to do the following:

- Send secure messages to Customer Service or Audit staff
- Submit a Part B redetermination
- Check status on any redetermination submitted to WPS GHA
- Enter a Part B claim
- Submit a Part B clerical error reopening
- Submit an overpayment claim adjustment
- Submit medical documentation
- Request duplicate remittances
- Request prior authorization for Hyperbaric Oxygen (HBO) services
- Submit electronic refunds
- Receive and respond to ADRs and Demand Letters

The Medicare Number field will accept either Health Insurance Claim Number (HICN) or a Medicare Beneficiary Identifier (MBI).
User Responsibilities, Access, and Management

User Responsibilities (All Users)

REPORTING A SECURITY INCIDENT
Users shall immediately report any known or suspected:
- Activity that violates the “CMS Information Security Policies, Standards, and Procedures”
- Activity that compromises information security
- Other suspicious activity

Please contact WPS GHA Customer Service with the following information:
- User Information:
  - User Login ID
  - National Provider Identifier (NPI)
  - Provider Transaction Access Number (PTAN)
  - Tax Identification Number (TIN/EIN)
- Date and Time the incident was identified
- Specific details of the security incident
- What steps, if any, have been taken by the User since the incident was identified

Please contact WPS GHA Customer Service at a number listed below:

MAC J5 Part A/B (IA, KS, MO, NE) and J5 National
(866) 518-3285

MAC J8 Part A/B (IN, MI)
(866) 234-7331

SHARING WPS GHA PORTAL USER LOGIN IDS
Every portal user must have their own User Login ID that is registered under their own name to adhere to privacy laws. Portal users cannot share their User Login ID. This means employers may not create a “Master” login and have all employees share that account. Each user must have their own account registered in their own name.

Access to the WPS GHA Portal
- Register as an NPI Administrator for a Medicare provider (by NPI). Be prepared with authentication criteria required through the registration process. As an administrator, you will be responsible for creating, approving, and maintaining the standard and eligibility accounts under you.
- Register as a non-administrator portal user and request access and approval by your NPI Administrator. Existing NPI Administrators can also create an account on your behalf.

REGISTER AS A WPS GHA PORTAL ADMINISTRATOR FOR A MEDICARE PROVIDER
Only two Administrators may self-register. If the NPI you are attempting to self-register for
already has two or more administrators, or you will not be an administrator, please follow the instructions “Request Access through your NPI Administrator” below to request access, then follow the instructions “Requesting Access for Additional Administrators” if you require Administrator level access.

- Access the portal at: http://www.wpsgha.com
- If you do not have an account, select the “Login/Register” button at the top right side of the page, then choose “Create Account” on the left-hand side.

- Read the details of the Transactional and General Areas of the User Agreement and select “I Accept” then select “I have read…” statement to continue the registration process then select “Next.” Selecting “Cancel” terminates the registration process and reverts back to the Home Page.
On the “Provider Credentials” page enter the National Provider Number (NPI), Provider Transaction Access Number (PTAN) and Provider Tax Identification Number (TIN/EIN) for the NPI you are requesting access for. When done select “Next.”

On the Financial Information screen read the details and select either “Yes” or “No” if you are the appropriate person to be the Administrator for this NPI. If “No” is selected, continue on in the registration process if there is already at least one administrator.

- If “Yes” is selected, click the “Next,” button and a pop-up with the WPS GHA
Portal Administrator Role Responsibilities will display.

- Review the Administrator Role responsibilities and select “Accept” or “Decline.”
- Selecting “Accept” will take you to the Financial Information screen to enter data to confirm authorized access to a Service Location.
- Selecting “Decline” will revert back to the Financial Information page to select “No” and continue with the Registration process.

**NOTE:** If there are no NPI Administrators for the NPI and you “decline” you will not be able to complete registration. Only two NPI Administrators can self-register for a user account and gain immediate access to the portal. It is the responsibility of the Administrator to create and approve access for additional users under their NPI.
  - If “Accept” was selected, the second page requests that you select one of the three tabs to verify your access to the service location. Enter the required data of your choosing (Patient Lookup, Medicare Check # or Medicare Claim #), then select “Next.”

**NOTE:** Selecting the “Back” button will revert back to the Provider Credentials page and selecting “Cancel” will cancel out the entire registration process and revert back to the Login/Registration page.

**NOTE:** Make sure that you verify that the NPI you are using for registration matches the financial information needed to complete the below step.

---

Are you the appropriate person to be the Administrator for this NPI?

- ☑ Yes - Are you the appropriate person to be the Administrator for this NPI?
- ☐ No - Someone else has that responsibility

**Confirm Financial Access to Service Location (NPI)**

You have 3 options to provide financial data to verify your access to this Service Location (NPI).

![Options](image)

Using a remit sent to this provider (NPI: [NPI]) in last 30 days (not dated older than [Date]) please enter:

**Check number from a Medicare payment:**

Check Number

For Part A claims, you may need to add or remove the leading zeros

---

- On the “About You” page, enter all required data to create a user account and then select “Next” when done.
- Provider Name
• Your Name  
• Email Address/Confirm Email Address  
• Phone Number  
• Work Location Name  
• Work Location Address (must be a street address, not a P.O. Box)  
• Create a permanent User Login ID. User Login IDs are 5-16 characters in length. (Spaces are not allowed)  
• Allowable characters include:  
  o A-Z  
  o 0-9  
  o Dollar ($)  
  o Underscore (_)  
  o Hyphen (-)  
• Review password rules prior to creating the password. To create a password, enter the password in “New Password” and enter the same password in “Confirm Password.”  
  o Portal password requirements  
    ▪ Passwords can only be changed once in a 24-hour time period  
    ▪ Passwords will automatically expire after 60 days  
    ▪ Passwords must be 8 - 20 characters in length  
    ▪ Passwords must contain at least:  
      • One upper case alphabetic letter: A - Z  
      • One lower case alphabetic letter: a - z  
      • One numeric digit: 0 - 9  
      • One special character (only the characters listed below are valid):  
        o Hashtag (#)  
        o Dollar ($)  
        o Percent (%)  
        o Ampersand (&)  
    ▪ Passwords cannot contain any of the following information:  
      • First or Last name  
      • Any special characters that are not listed above  
      • User Login ID  
      • Security question answers  
      • Words (words consisting of four or more letters) Please note: This is the requirement most often overlooked and causes the most difficulty for users. To successfully create a password, please avoid “dictionary” words. (EXAMPLES: Book, Tree, Water, etc.).  
      • Newly created passwords must be different than the previous 24 passwords used.  
      • Newly created passwords must differ from the previous password by at least four characters.  
• You may also choose to have the portal auto-generate a password for you. If the “Generate Password” link is selected, the portal will generate a password and will auto fill in the “New Password” and “Confirm Password” fields.  
  o Please remember the generated password as this will be needed the next time you log in.  
• For a second level of security (E-Signature) enter your date of birth and select and answer three questions, select “Next.” The only time you will use your date of birth and security questions are when you are using the Forgot User Login ID/Password feature
and for recertification of your portal account.

- You will receive Confirmation showing that registration was successful, and you can log in to the portal by selecting the "Login" button.

REQUEST ACCESS THROUGH YOUR NPI ADMINISTRATOR

- Repeat the first 4 above.
- On the Financial Information page, if it states there are already two or more Administrators, or there is only one, but you do not hold that responsibility and choose the option for “No,” you will be requesting access through the current NPI Administrator. Choose “Next.”
- **Note:** If there are no current Administrators and you will not become one, someone who will be an administrator must register first.
- On the “About You” page, enter all required data to create a user account and then select “Next” when done.
- Provider Name
- Your Name
- Email Address
- Confirm Email Address
- Phone Number
- Work Location Name
- Work Location Address (must be a street address, not a P.O. Box)
- Next, create a permanent User Login ID. User Login IDs are 5-16 characters in length. (Spaces are not allowed)
- Allowable characters include:
Review password rules prior to creating the password. To create a password, enter the password in “New Password” and enter the same password in “Confirm Password.”

**Portal password requirements**
- Passwords can only be changed once in a 24-hour time period
- Passwords will automatically expire after 60 days
- Passwords must be 8 - 20 characters in length
- Passwords **must contain** at least:
  - One upper case alphabetic letter: A - Z
  - One lower case alphabetic letter: a - z
  - One numeric digit: 0 - 9
  - One special character (only the characters listed below are valid):
    - Hashtag (#)
    - Dollar ($)
    - Percent (%)
    - Ampersand (&)
- Passwords **cannot contain** any of the following information:
  - First or Last name
  - Any special characters that are not listed above
  - User Login ID
  - Security question answers
  - Words (words consisting of four or more letters) **Please note:** *This is the requirement most often overlooked and causes the most difficulty for users. To successfully create a password, please avoid “dictionary” words. (EXAMPLES: Book, Tree, Water, etc.).*
  - Newly created passwords must be different than the previous 24 passwords used.
  - Newly created passwords must differ from the previous password by at least four characters.
- You may also choose to have the portal auto-generate a password for you. If the “Generate Password” link is selected, the portal will generate a password and will auto fill in the “New Password” and “Confirm Password” fields.
  - Please remember the password as this will be needed the next time you login.
  - For a second level of security (E-Signature) enter your date of birth and select and answer three questions, select “Next.” The only time you will use your date of birth and security questions are when you are using the Forgot User Login ID/Password feature and for recertification of your portal account.
- You will receive Confirmation showing that registration was successful, and you can log in to the portal by selecting the “Login” button.
- If you attempt to log in before approval has been granted by the NPI Administrator, you will receive the message “Your account is currently pending approval by the NPI administrator. You can go to the help center for more information or continue in the public site.”
REQUESTING ACCESS FOR ADDITIONAL ADMINISTRATORS (MORE THAN TWO)
Only two individuals may self-register as an NPI administrator. If there is need for additional administrators, the person requesting administrator access must first register for a regular user account if they do not currently have any access. After registration and approval, send a secure message requesting that the specific user be brought to the administrator level. You need to include the User Login ID, User’s full name and what NPI they should be Administrator for.

LOGGING IN
- Access the WPS GHA Portal at: http://www.wpsgha.com
- Click on the “My Account” tab or the “Login/Register” button.
- Enter your User Login ID, password, Date of Birth, and answer to the Secret Question.
- Select “Login.”
- User’s “Dashboard” page is presented to begin approved portal activity.

Logging in after “X”ing out of WPS GHA Portal versus selecting Log out

If a WPS GHA Portal user selects the “x” in the top right-hand corner of the webpage to log out of the WPS GHA Portal they may encounter the following error when trying to log back in: “DPWNS1056W You are already logged in from another client. Do you want to terminate your existing login or cancel this new login request?”

The user will have two links available to choose from “Terminate existing login” and “Cancel this new login.” The User should select “Terminate existing login.” This will terminate the previous
session that was not properly logged out of and allow the User to sign in again. To properly log out of the portal, click on the gear icon next to your name and then click “Logout.”

Logging Back in After Timeout Issues

Many times, when a WPS GHA Portal user has been logged out after 15 minutes of inactivity, they report difficulty logging back into the Portal. One of the simplest fixes for this issue is for the WPS GHA Portal user to do the following steps:

- Close all open website browsers (not just the WPS GHA Portal site).
- Reopen the website browser and manually enter the link: https://www.wpsgha.com
- If the login still gives an error, on the logout link (if available), and if that is not showing, then follow the Clearing Cache steps above, close all browsers and try again.

MULTI-FACTOR AUTHENTICATION

Multi-Factor Authentication (MFA): a CMS requirement that provides an additional form of security to safe guard your doctor and patient information. When logging into the portal, you will request and enter an MFA Verification code that you will obtain one of three ways:

- Email
- Phone Call (cannot use a phone number that has an extension)
- Google Authenticator Application.

Note: Your Date of Birth and Secret Questions are still an integral part of the WPS GHA portal. These will be needed when using features such as Forgot User ID, Forgot Password and Recertification. Please assure you remember the selections you make as you use the portal.

The MFA process will auto populate the email and telephone with values that are currently listed on your profile page. Even though both Email and Telephone options are populated on the MFA set-up page, you are not required to use both or verify both options. If you choose to verify only one option, that is fine, but verifying both gives you a backup in case you can’t get the code thru one option.
Follow the steps below to get set-up for MFA.

- Click Continue.
- Initially, you will be able to set up email and phone to receive the MFA verification code. Click on the Setup Email & Telephone box

Steps to set up your email

- Enter your Email address in the appropriate box (or verify the Email address pre-loaded is the one you want to use to receive the MFA code). Click the Send Code button.
Obtain the MFA Verification code from the email sent to the Email address you indicated above. Be aware, this code will expire 1 hour after being sent, so you must log in to use the code within 1 hour otherwise you will need to request a new code. Once you enter the code in the Verification Code box and click "Verify Code," the code will be valid for 12 hours. Once it has been verified you will see a check mark next to the email address.
If you are having trouble receiving the email, or the code did not work, and you want to try a new code, click on the “Back to Previous Step” link. This will take you back to Step 5 of this manual.

Steps to set up your telephone Number

- We encourage you to set up the phone option as well as a backup to email. If you also choose to set up for Phone verification, enter the phone number that you will use to receive the Verification code. If the phone number pre-loaded is not the one you want to use update the field with a new phone number. Please note that this cannot be a phone with an extension. It must be a direct dial number and can be a cell phone number.

Click the Send Code button if you are ready to validate the phone number. (If you do not want to validate your phone number now and only use Email as your verification, click on the Continue button and skip to Step 11 of this Manual.)
An automated phone call will be made from WPS GHA with the following message:
“Hello. Thank you for using the WPS GHA Multi-Factor Authentication phone verification option. Your code is: [randomly generated six-digit number] Again your code is: [repeat of six-digit number]. Remember, you should not share this code with anyone else, and no one from WPS GHA will ever ask for this code. Goodbye.” Enter the code obtained in the phone call in the Verification Code box and click “Verify Code.” Once the code is verified you will see a check mark next to the telephone number. As with the email option, please be aware, this code will expire 1 hour after being sent, so you must log in to use the code within 1 hour otherwise you will need to request a new code. Once you enter the code in the Verification Code box and click “Verify Code”, the code will be valid for 8 hours. Once it has been verified you will see a check mark next to the Telephone number.

- Click Continue to set up your primary (default) option.
- Choose which option you want to use as your default or primary choice. You can change this selection at any time. If you did not verify the phone number, the email address will be pre-selected as the default. Once you selected your default, click “Finish.”
You will receive a message at the top of the screen that you have successfully set up your Multi-Factor Authentication.

A third option to receive an MFA Verification code is use of Google Authenticator. Google Authenticator is an application that implements two-step verification and is an app typically installed on a smart phone. This is not a required method but is a very useful method for meeting the Multi-Factor Authentication requirement. To use Google Authenticator, first download the app via Google Play or the App Store. Follow the steps on the app to download to your phone.
Once you have installed Google Authenticator to your phone, use the application to scan the Bar Code in the WPS GHA portal (shown below). You will receive a Verification Code on your phone. Enter that code in the Verification Code box and click “Verify.” If you choose to use this method as your default, select the box. Please note: the code must be entered within 30 seconds from the time it is displayed in the Authenticator app.

You will receive a message that you have successfully enabled the Google Authenticator app.
Once you have set up your Multi-Factor Authentication you will be taken to your Dashboard.

The next time that you log into the portal, you will enter your User Login ID, Password. Obtain and enter a new authentication code using any of your validated choices. You will no longer enter your date of birth and Secret Question to log in.

Once you have logged in using your verification code, if you log out and need to log in again, remember, you will not have to request or enter your code again. You will see the below screen.
Changing Default option to Google Authenticator

When your MFA default option is email, or Phone and you want to change it to Google Authenticator follow the below steps:

- Login to the portal and go to “My Profile” page.
- Click on MFA button.
- Click on Setup Google Authenticator box
- Click on “Set as Default” box.

How to Change your Email Address or Phone Number for MFA

You can change your email address and/or phone number any time after setting up your MFA access. Follow the below steps to change/update.

- Log into the portal with your User Login ID and password.
- You will need to request a code be sent to either your Email or Telephone.
• After you obtain your code and log into the portal and are on your Dashboard,
  o Click on the “My Profile” link in the left-hand navigation
  o On the My Profile page, click on the MFA tab at the top of the screen.
  o On the Multi-Factor Authentication page select the option that you are changing
  o Enter in the correct value (Email address or Phone number)
  o Click Send Code
  o Obtain the verification code from either your Email or Telephone
  o Enter Code and click Verify and Finish.
  o Once it is changed you will receive message at the top of the page “You have successfully updated your Multi-Factor Authentication methods”

Logout

To logout of the portal select the gear icon at the top of the page next to your name. A dropdown box will display, click Logout.

RECERTIFICATION

Annually, users must recertify all active User Login IDs that have access to the portal. Notifications are presented in the portal 90 days prior to the recertification date to allow adequate time to complete the recertification steps. The recertification process is very similar to registration. If a User fails to complete the portal recertification process timely, access is disabled. Once access is disabled a user will need to complete the registration process as a new user.

• Access the portal at: http://www.wpsgha.com
• Once Recertification is due within 90 days, the user will receive the Recertify pop-up window on the “My Dashboard” page. Choose “Recertify” from the pop-up, or, from the “My Dashboard” page click on your username in the top right, and if Recertification is due, there will be an option for “Recertification.”
- Read and accept the transactional and general terms of use. Then choose “Next.”

**Terms of Use for Transactional Areas**

To continue, you must read and accept the following agreements.

- **Transactional**
  - I accept

- **General**
  - I accept

I have read and agree to abide by these Terms of Use for Transactional Areas. I understand that acceptance provides Medicare with an electronic signature.

- The WPS GHA portal requires all users to attest that you have or will be completing your company’s annual security awareness training. If you select no, your account will be permanently disabled. Then choose “Next.”
- Enter the provider credentials for any one of the Service Locations (NPIs) you currently have access to. Then choose “Next.”

- Enter your choice of financial information, from the last 30 days. Then choose “Next.” You can enter:
  - Patient Medicare number and Date of Service
  - Medicare Check Number
  - Medicare Claim Number
- **NOTE:** Make sure that you verify that the NPI you are using for registration matches the financial information needed to complete the below step.
Review and update your personal information, then choose “Next.”

E-Signature Verification
- In order to recertify, three new security questions must be selected and answered.
- Once complete, select “Next.”

Recertify Admin Role
- Administrators must recertify NPI Administrator Role Responsibilities. Only NPI Administrator Users will need to reaccept the Admin role.
  - Verify the listed NPIs and review the Administrator responsibilities.
  - Select “Reaccept Admin Role” to continue recertification.
- If you choose to modify your access to any NPI, go to “My Service Locations.” Once this is done, the Re-Certification process will need to be done again and “Finish” must be selected when completed.

You will receive a Recertification complete message. Select “OK.”

Account Reactivation

User’s Account

If a user account has been disabled for any reason, an NPI Administrator has the ability to reactivate the account. Once access is disabled, a user must contact their NPI Administrator to request their account be reactivated.

Note: Only accounts disabled after 04/17/2019 can be reactivated. Accounts that have been disabled for more than 1 year from their disabled date cannot be reactivated.

Administrators Only
- Access the portal at: http://www.wpsgha.com
- Click on the Reactive User button on your User Administration page
• Enter the following information (Note: This information must match what is on the user’s account):
  o User Login ID
  o User First Name
  o User Last Name
  o User's Email Address
• Click “Submit”

• Click “Confirm” on the confirmation pop-up box
• The Administrator will receive the message “The account has been successfully reactivated.” and an email.
• The reactivated user will also receive an email

Administrator’s Account

If an Administrator’s user account has been disabled for any reason, the Administrator has the ability to reactivate their own account.

Note: Only Administrator accounts disabled after 08/08/2019 can be reactivated. Accounts that have been disabled for more than 1 year from their disabled date cannot be reactivated.
Administrators Only

- Click on the “Is your NPI Admin Account expired?” link in the Secure Login box under the “Forgot User Login ID/Password?” link

- Enter the following information (Note: This information must match what is on your account):
  - User Login ID
  - Date of Birth
  - Select one of your Secret Questions from the drop down
  - Secret Answer
  - NPI for the financial data
  - Financial Data for one of the tabs; Patient Lookup, Medicare Check # or Medicare Claim # that matches the NPI you entered

- Click “Submit”
Administrator - Self Reactivation

Your account has been disabled. As an Administrator you can reactivate your own account by completing the below information. Enter your account information: User Login ID, Your Date of Birth, Choose one of your Secret Questions and the Answer, NPI and one of the 3 options of Financial Information. This will reactivate your account. You and any other administrator(s) for NPI that you have access to will receive an email confirming that your account has been reactivated. If you have entered all information correctly, you will get a confirmation email and your account would have been reactivated.

User Login ID

User Login ID*: Username

e-Signature

Date of Birth*: mm/dd/yyyy

Secret Question*: Secret Question

Secret Answer*: 

Financial Information

You have 3 options to provide financial data to verify your access to this Service Location (NPI).

NPI (Service Location)*: NPI(Service Location) for the below financial information

Patient Lookup | Medicare Check # | Medicare Claim #

Using a remit sent to this provider in last 30 days (not dated older than May 26, 2019) please enter:

Patient's Medicare Number*: Patient's Medicare Number

Max 02 characters

Date of Service*: mm/dd/yyyy

Submit | Clear
• You will receive the following pop-up box

Administrator - Self Reactivation

If you do not receive a confirmation email, please verify the information and try again. If the information provided was valid your account will be reactivated. You and any other administrator(s) for the NPIs that you have access to will receive an email confirming that your account has been reactivated. Once reactivated you will need to re-certify your account in 1 year.

Check For Confirmation Email

Login
Need to resubmit?

• Check your email for a confirmation email that your account was reactivated
• If you did not receive an email then at least one piece of the data you enter was incorrect and you can try again by clicking on the “Need to Resubmit?” link
• If your account was reactivated then all other Administrators for the NPIs that you have access to will also receive an email

Username/Password Management

INITIAL PASSWORD
User passwords are created during the registration process. Both an administrator and self-registering user will create their own passwords, however, a user account that is created by an administrator will get a temporary password emailed to them to the email address on file within the Portal. The initial password is a one-time use only password valid for 21 days. Once it has been entered, a new password will need to be created. If the password is not used within the 21 days, the new account will no longer be valid, and a new account will need to be created.

PASSWORD REQUIREMENTS
The Centers for Medicare & Medicaid Services (CMS) and WPS GHA are committed to protecting the health information of Medicare beneficiaries. To ensure this level of protection, WPS GHA is dedicated to meeting the CMS security requirements.

Portal password requirements
• Passwords can only be changed once in a 24-hour time period
• Passwords will automatically expire after 60 days
• Passwords must be 8 - 20 characters in length
• Passwords must contain at least:
  o One upper case alphabetic letter: A - Z
• One lower case alphabetic letter: a - z
• One numeric digit: 0 - 9
• One special character (only the characters listed below are valid):
  ▪ Hashtag (#)
  ▪ Dollar ($)
  ▪ Percent (%)
  ▪ Ampersand (&)
• Passwords cannot contain any of the following information:
  ▪ First or Last name
  ▪ Any special characters that are not listed above
  ▪ User Login ID
  ▪ Security question answers
  ▪ Words (words consisting of four or more letters) *Please note: This is the requirement most often overlooked and causes the most difficulty for users. To successfully create a password, please avoid “dictionary” words. (EXAMPLES: Book, Tree, Water, etc.).*
• Newly created passwords must be different than the previous 24 passwords used.
• Newly created passwords must differ from the previous password by at least four characters.
• Make sure all check marks on the right side of the page are green. If they are not all green, make the necessary correction(s).

Some helpful suggestions to assist you in the creation of your new password are listed below or see next section about auto-creating a password.
• Choose a smaller password and repeat it: Ab#1Ab#1
• Use the $ sign instead of the letter “S”: Pa$$1Pa$$1
• Use the number zero instead of the letter “O”: w0rd1w0rd1
• Use the number one instead of the letter “I”: Wh1te$Wh1te$

**AUTO CREATED PASSWORD**
You may elect to have the Portal create a password for you by selecting “Generate Password.” Once selected, the password will auto fill in both the “New password” and “Confirm Password” boxes. Please remember the password as this will be needed the next time you log in.

**EXPIRED PASSWORD**
If the User password has expired, the Password Expired page will display upon login.
• Enter the expired password in the “Current Password” field.
• Enter a newly created password in the “New Password” field.
• Enter the newly created password again in the “Confirm Password” field.
• Select “Save my password” in the bottom right hand corner.

Please remember the password as this will be needed the next time you log in.

**FORGOT USERNAME/PASSWORD**
Usernames are created during the registration process. If you have forgotten your Username or Password, follow the below steps:
• From the main Portal page select the “Forgot User Login ID/Password?” link.
Select either “I don’t know my User Login ID” or “I don’t know my Password,” whichever is appropriate for the situation?
Enter the requested information:
  - For User Login ID enter:
    - Email Address
    - NPI number
    - Date of Birth
    - Secret Question
    - Secret Answer
    - Choose “Retrieve User Login ID”

In order to retrieve your User Login ID, please enter an NPI that you currently have access to, your registered date of birth, and one of your 3 secret Q&As. If the data matches, we’ll send you your User Login ID to the registered email in your account.

For Password enter:
  - User Login ID
  - Choose “Lookup My ID”

To reset your password, please start by entering your User Login ID below.

Next Enter:
  - Date of Birth
  - Secret Question
  - Answer to Secret Question
  - Choose “Reset Password”
Once “Retrieve User Login ID” or “Reset Password” has been selected, a message will display stating “Please check your email for your User Login and/or temporary password.” This is the User’s email address that is currently on file within the portal.
- Please ensure you check your spam and junk email folders as well.

Login to the WPS GHA Portal with your User login ID and/or the temporary password from the email. If you reset your password, the Password Expired page will display upon login.
- Enter the temporary password in the “Current Password” field.
- Enter a newly created password in the “New Password” field.
- Enter the newly created password again in the “Confirm Password” field.
- Select “Save my password” in the bottom right hand corner.
- The temporary password is a one-time use only password valid for 21 days. Once it has been entered, a new password will need to be created. If the password is not used within the 21 days another password reset will need to be done.

Please remember the password as this will be needed the next time you log in.

**Locate Administrator to Update Your Account**

Occasionally there may be a need to contact your NPI Administrator for various tasks, such as resetting your password or secret Q&As or updating your profile in some way. To find your Administrator(s), follow the steps below.

- When logged in:
  - Click on the “My Service Locations” link in the left navigation.
  - Scroll to “My Service Locations (NPIs).
  - Find the NPI in question.
  - Click on the blue “Find My Admin” button under the Admin? Heading.
  - Pop-up will appear with the Location NPI, PTAN and TIN and Display the Name, Phone and Email for the Administrator.
If not logged in, on the Secure Login page, go to the NPI Administrator Search box and enter the full NPI, PTAN, and Tax ID, then choose “Submit” to perform the search or “Clear” to start over.

If you have not received approval to a location request and need to know who the NPI Administrator is:
- Click on the “My Service Locations” link in the left navigation
- Scroll to “My Pending Access Requests.
- Find the NPI in question.
- Click on the blue “Find My Admin” button under the Admin? Heading.
- Pop-up will appear with the Location NPI, PTAN and TIN and Display the Name, Phone and Email for the Administrator.
• A list of all active NPI Administrators for the NPI information you entered will be returned. The information will include their name, phone number, and email address on file. Use this information to contact them to make your request.

Contact NPI Administrator

Login Error

If you are already logged into the portal and just “x” out to close and then try to log in again, you will receive the below error. You will need to choose to either terminate the existing login or cancel the new one.

You are already logged in from another client.

Do you want to terminate your existing login or cancel this new login request?

Terminate existing login  Cancel this new login
My Account Tools

**MY DASHBOARD**
When you log in, you will always land on the “My Dashboard” page. You will see a left navigation section, as well as some dashboard “windows.” Both the left navigation bar as well as the “My Dashboard” windows may vary upon your access level. Administrators have full access, standard users have access to the non-admin functions of the portal, while eligibility users can only access their own account and the “Eligibility Check” transaction.
USER DASHBOARD WINDOWS
Depending on what level of access you have (Administrator, Standard user, Eligibility only user) there will be different features on your dashboard.

Users at the Administrator level will have all four dashboard windows, “Pending Access Requests,” “Registration Approvals,” and “Blackout NPIs.” Users at the Standard or Eligibility only level will be able to access only one of the Dashboard windows, “Blackout NPIs.”

PENDING ACCESS REQUEST (ADMINISTRATORS ONLY)
This window will display the number of pending access requests that you have waiting for approval. These are requests for access to NPIs that you administer.

- If there are requests in the “Pending Access Requests” window, select “Go to User Requests.”
- Select the “Pending Access Requests” tab.
• Scroll to the request and select “Show Request.”

![Image showing a portal entry with details]

- Grant access to all NPIs that have been requested. Use the “Change all NPIs to” radio buttons along the top to give the same access to all NPIs or use the radio buttons to the right of each individual NPI to customize the access for each NPI. Select Eligibility, Standard, or No Access (Deny Access) for the user.
  - Click “Save changes.”

![Image showing a service location request form]

• On the Confirmation, verify information and then select “Save.”

A message at the top of the page will be received stating “Service Locations (NPIs) successfully updated.”
REGISTRATION APPROVALS (ADMINISTRATOR ONLY)
This window will display the number of pending registration requests that you have waiting for approval. These are requests for first time registrations.

- If there are requests in the “Registration Approvals” window, select “Go to User Requests.”

- Select the “Registration Approvals” tab.

- Scroll to the requests and select “Show Request”

- On this page, you can grant access to all NPIs that have been requested. Use the radio buttons to the right of the NPI to customize the access for each NPI. Select Eligibility, Standard, or No Access (Deny Access) for the user.
  - Click “Save changes.”
On the Confirmation, verify information and then select “Save.”

A message at the top of the page will be received stating “User successfully approved.”

**BLACKOUT NPIs**

This window will display the number of NPIs in Blackout status. There must be an NPI Administrator for each NPI location. If all Administrators for an NPI lose or remove their access to an NPI, the NPI will go into “Blackout” status. If there is not a user willing or able to become the Administrator, all users under that NPI will lose access to that NPI after 30 days of being in blackout status.

- If there are NPIs in the “Blackout NPIs” window, select “Go to My Service Locations.”

When there is not an NPI Administrator you will receive the following message:
- “The following Service Locations (NPIs) have a Blackout Status. This means that they don’t have an active Administrator on record. If you want to become an Administrator, click on the “Accept Role” button and provide the appropriate financial information.”
- Scroll to the NPI that is listed as not having an Administrator, select “Accept Role” if you will assume Administrator responsibility.
Read and accept the WPS GHA Portal Administrator Role Responsibilities by selecting “Accept Role” button.

On the Confirm Financial Access for Service Location (NPI) Administration, select one of the three options for providing financial data.

**Confirm Financial Access to Service Location (NPI)**

You have 3 options to provide financial data to verify your access to this Service Location (NPI).

- **Patient Lookup**
- **Medicare Check #**
- **Medicare Claim #**

Once entered, select “Confirm.”

**User Search (Administrators Only)**

For NPI Administrators only, below the Dashboard windows, there is a “User Search” area. In this section, you will be able to do a search for any users that you administer under your NPI(s). If you know the User Login ID for the user you can enter that, select “Go to User Profile,” and be taken to their Profile page. You may also select “Find More Users” to bring up additional options for searching.
QUICK LINKS
On the Dashboard page, there are Quick Links that will take you directly to a function. Your links may vary depending on your access.

NEW MESSAGES
On the Dashboard page, there is a “New Messages” section that gives you a quick overview of new messages. You may go directly to the “Message Center” or open the individual messages by clicking the Tracking Number link.
My Profile

Your Profile page consists of your User Login ID, personal information, and the Billing Provider Credentials that you used during registration.

There are several Profile Actions that can be performed from the “My Profile” page.

**CHANGE MY PASSWORD**
To change your password at any time (limit of once per 24 hours):

- Choose “My Profile” from the left navigation.
- Select “Change My Password.”
- Enter the current password in the “Current Password” field.
- Enter a newly created password in the “New Password” field.
- Enter the newly created password again in the “Confirm Password” field.
- You may also opt to have the portal auto-generate a password by choosing the
“Generate Password” link. This will auto-fill the password into the required fields. Please remember the password as this will be needed the next time you log in.

- Select “Save my password” in the bottom right hand corner.

Current Password *

New Password *

Confirm Password *

**CHANGE SECURITY Q&As**

To change your security questions at any time:

- Choose “My Profile” from the left navigation
- Select “Change Security Q&As”
- Choose and answer three new questions
- Select “Save Changes”
- After the changes have been saved, a message will be received stating “Your security questions have been successfully updated.”

Security Questions
DISABLE MY ACCOUNT
To disable your account at any time:

- Choose “My Profile” from the left navigation.
- Select the “Disable My Account” button
- On the “Disable My Account” pop-up box select “Disable.” Otherwise select “Cancel” to return to your “My Profile” page.
- The page will refresh and display a message indicating the account has been disabled successfully.

MY SERVICE LOCATIONS
Use this page to view, manage, and modify the Service Locations (NPIs) that you have access to. If Blackout or Pending Locations are available, they will display on this page. You can also request access to a Service Location (NPI) that you do not have access to.

- Request Access to additional NPI locations with the “Request Access” button.
  - The NPI location’s current Administrator will receive your request and decide whether to approve and at what level of access, or to deny access altogether.
  - If there are is no current administrator, you will be prompted to accept the role.
- Find current NPIs under “My Service Locations (NPIs)” section either by scrolling through the NPIs or enter the NPI in the “Filter” box.
- Modify access if your access is currently at an Administrator level for that NPI
- Remove the access
- Select “Save Changes” when finished.
Message Center

The Message Center is a secured communications channel that currently allows users to submit confidential inquiries directly to the Provider Contact Center (PCC) or Audit department. The Message Center will be expanded in the future to allow additional submissions such as a response to a development letter or a demand letter.

Upon initial selection of the Message Center from the left navigation the page will load your message center history. If you have a large volume of messages in history, it may take a while to retrieve and display your messages. Please be patient.

- Examples of inquiries to the Provider Contact Center include complex policy questions or claim denials, inquiries that you are currently familiar with submitting via the portal. Provider Contact Center inquiries sent via Message Center are considered written inquiries and Medicare has up to 45 business days to respond to your inquiry. Responses will be available in the Portal once the PCC has completed the inquiry.
- Examples of an Audit submission include submission of Cost Report supporting documentation or a Cost Report Reopening request. The Audit area will contact you if
additional information is needed on your request.

**SEND A SECURE MESSAGE**

- Select the link “Message Center” on the left-hand navigation bar
- On the Message Center page, select “+ New Message”

---

**CUSTOMER SERVICE**

- Complete the required fields marked with an asterisk (*):
  - Registrant Name (auto populated from Profile)
  - Email Address (auto populated from Profile)
  - Service Location NPI that pertains to our inquiry.
  - Category
**New Message**

Use this page to contact Customer Service through a Secure Message. Make sure you select the appropriate type of question on your query. They are:

- **Technical Question.** A question or issue that pertains directly to the use or functionality of the WPS GHA Portal. Examples include adding or removing locations, adding or removing users, site navigation, and understanding screen information.
- **Non-Technical Question.** A question or issue that does not directly pertain to the WPS GHA Portal. Examples include policy questions or clarification on claim denials.

CMS allows contractors 45 business days from the date of receipt to respond.

Required fields are marked with an asterisk (*).

<table>
<thead>
<tr>
<th>Field</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider Transaction Access Number (PTAN)</td>
<td>XXX-XXX</td>
</tr>
<tr>
<td>Last 5 digits Provider Tax Identification Number (TIN/EIN)</td>
<td>XXX-XXX</td>
</tr>
<tr>
<td>Phone number*</td>
<td>Area [Local Phone] Ext</td>
</tr>
<tr>
<td>Type of Question*</td>
<td>Please Select</td>
</tr>
<tr>
<td>Subject*</td>
<td></td>
</tr>
<tr>
<td>Description*</td>
<td>10,000 character maximum. You have 10,000 characters left.</td>
</tr>
</tbody>
</table>

- Enter Provider Transaction Access Number (PTAN)
- Enter Last 5 digits of the Provider Tax Identification Number (TIN/EIN)
- Enter Telephone Number
- Select the Type of Question
  - Technical – A question or issue that pertains directly to the use or functionality of the WPS GHA Portal. Examples include adding or removing locations, adding or removing users, site navigation, and understanding screen information.
  - Non-Technical – A question or issue that does not directly pertain to the WPS GHA Portal. Examples include policy questions or clarification on claim denials.
- Enter Subject (We suggest a subject that will allow you to easily locate the response in the Portal)
- Enter your question in the Description area in as much detail as possible to allow...
for adequate research of your inquiry. You may enter up to 10,000 characters. Include details such as the ICN, date of service, beneficiary information, etc. The Portal is a secure environment, so you are allowed to include PHI/PII in your inquiry.

- Select “Continue”
- Once submitted, a confirmation page will display the details of the inquiry. To make corrections select “Cancel” or to submit the request select “Save.”

Once saved, you will receive a Secure Message Confirmation screen that provides a Tracking number for the inquiry.

- Please keep this Tracking number for future use or print this page for reference as the Tracking number is needed to go back and view the response.

**Secure Message Confirmation**

Message successfully sent. Tracking Number: k1534375212863

Thank you for your request. Your request has been submitted and assigned the tracking number shown above.

**Message View / Print**

Login ID: [redacted]  |  NPI: [redacted]  |  Type: Technical
Submitter Name: [redacted]  |  PTAN: [redacted]  |  Client Status: Sent
Submitter Email: [redacted]  |  TIN: [redacted]  |  CSR Status: Received
Submitter Phone: 508111111  |  State: MI  |  Submitted Date: 08-15-2018
Case #: [redacted]  |  Medicare Plan Code: A  |  Status Date: 06-15-2018
Closed:
AUDIT

- Complete the required fields marked with an asterisk (*):
  - Registrant Name (auto populated from Profile)
  - Email Address (auto populated from Profile)
  - Service Location NPI that pertains to our inquiry.
  - Sub Category
    - Audit Advisement/Miscellaneous Issues
    - Cost Report Reopening
    - Cost Report Appeal
    - Rate Review
    - Wage Index
  - Provider Transaction Access Number (PTAN)
  - Fiscal Year End
  - Appeal Case # (only for Cost Report Appeal messages)
  - Enter Subject (We suggest a subject that will allow you to easily locate the response in the Portal)
  - Enter your question in the Message area in as much detail as possible to allow for adequate research of your inquiry. You may enter up to 10,000 characters. Include details such as the ICN, date of service, beneficiary information, etc. The Portal is a secure environment, so you are allowed to include PHI/PII in your inquiry.
  - Contact Person information (if not submitter)
  - WPS Contact information
  - Upload Attachment (accepted file types: DOCX, XLLSX, PDF, JPG, JPEG, GIF, TIF, TIFF, ZIP, DBF) Note: If you need to submit more than one file, they must be uploaded in a ZIP file. Files cannot be password protected.
  - Select “Continue”
  - Review Confirmation, if correct
  - Click “Save”
  - Print if needed by clicking the blue Print button.
New Message

Please select your NPI and appropriate Category message. In order to complete your new message into the Audit message center, please select your Sub Category from the below dropdown box and then complete all required (*) fields.

Registain name:* 
Email address:* 
Service Location (NPI)* 

Category:* 
Audit

Sub Category:* 
Audit Advice/Miscellaneous issues
Cost Report Reopening
Cost Report Appeal
Rate Review
Wage Index

PTIN:* 
Fiscal Year End:* 
Appeal Case#: 
Subject:* 

Message:* 10000 character maximum. You have 10000 characters left.

Contact Person (if not submitter):
First Name: 
Last Name: 
Email Address: 
Confirm Email Address: 
Phone Number: 

WPS Contact:
First Name: 
Last Name: 
Email Address: 
Confirm Email Address: 

Attachments
Accepted file types: DOCX, XLSX, PDF, JPG, JPEG, GIF, TIF, TIFF, ZIP, DBF.
Upload scans, pictures, screenshots or documents of claim forms, receipts, invoices or any other documentation needed to support your privacy.
Browse...
Once submitted, a confirmation page will display the details of the inquiry. To make corrections select “Cancel” or to submit the request select “Save.”
CHECK MESSAGE CENTER STATUS

Customer Service:
- Select the link “Message Center” from the left navigation
- Messages can be Sent or Received status.
- Sent status indicates that a secure message has been sent, but WPS GHA customer service has not yet responded to that message.
- Received status indicates that a secure message has been submitted and now has “Received” an answer from WPS GHA customer service.
- Delete status indicates that customer service responded to the message via telephone.
- On the Message Center page, select the case number link to view the responses from the Customer Service department.
- Once you have read the message you can either select “Print Message” or “X” out of the page.

Audit:
- Select the link “Message Center” from the left navigation
- Submitted status indicates that the message has been received in the portal.
- Completed status indicates when the message has been completed and a response returned to the portal user.
- Pending status indicates that WPS has sent a message that may require your response.
- Not Accepted status is when the message is accepted in the portal, but the attached file has a virus or is corrupt.
- You can click on the Tracking Number link to see the details of your message.

SEARCHING FOR A MESSAGE

Once you select the Message Center from the left navigation, you can search or refine your message history multiple ways.
- Quick Filter by Category, Tracking Number or by messages submitted by you. NOTE: with the new message center you will be able to see Audit messages submitted by other users that may have access to your NPI(s).
- Advanced Filter selections vary based on the Category selected (see below screens).
Advanced Filter when selecting All Categories:

Advanced Filter when selecting Audit only:
Advanced Filter when selecting Customer Service only:

User Administration (Administrators only)

As a WPS GHA Portal Administrator, you agree to perform the following activities within WPS GHA Portal.

Identity Proofing – the Administrator must verify the identity of all WPS GHA Portal User Account applicants within their NPI using a government issued identification document containing a photograph (e.g., driver license, passport, State ID card, etc.).

Registration – New accounts can be created by the NPI Administrator or by the User through the registration process. All new User access must be approved by an NPI Administrator.

Requesting Additional NPI Administrators – The Administrator is required to request access for additional NPI Administrators through the Secure Message functionality within the WPS GHA Portal. Please submit the following information:
- Indicate that you would like the user to have the NPI WPS GHA Portal Administrator access.
- WPS GHA Portal User Login ID (User must have a current ID)
- User’s First and Last Name
- NPI(s) the user should have Administrative access to

Access Requests – the Administrator must approve/deny requests for access to PII/PHI data within their NPI.

Re-Certification – the Administrator must ensure that all User Accounts under their NPI complete annual re-certification within 358 days.

Account Reactivation – if a portal user account becomes disabled for any reason, the Administrator can reactivate the account. Note: Only accounts disabled after April 17, 2019, can be reactivated. Accounts that have been disabled for more than 1 year from their disabled date cannot be reactivated.
**Reactivate Own Account** – the Administrator can reactivate their own account if it becomes disabled. Note: Only accounts disabled after April 17, 2019, can be reactivated. Accounts that have been disabled for more than 1 year from their disabled date cannot be reactivated.

**Maintenance** – the Administrator is responsible for maintaining user currency within their NPI as it applies to WPS GHA Portal User accounts.
- Add a new user account for new employee
- Remove location access for terminated employee. Disabling is not allowed.
- Adding/removing NPI location access per User
- Modifying user access level (Standard, Eligibility only, Administrator)
- Profile updates
- Password reset
- Clear Secret Questions and Answers

The NPI Administrator is also responsible for completing thorough user review every 90 days to assure all active accounts are in compliance. The NPI Administrator’s user review shall include the following steps:
- Verifying all active user accounts listed for each of the NPI’s he/she administers have appropriate Portal role access (Standard or Eligibility Only) and correcting if necessary.
- Verifying all active user accounts are current employees or members of the NPI organization and that the user should still have access to the WPS GHA Portal.
- If a user is no longer employed for the associated NPI, disabling the user account or removing the NPI location access immediately.

**Inactivity** – the Administrator must be aware that inactive User Accounts will automatically age off of the WPS GHA Portal and become disabled. Once disabled, the User will need a new account to access the WPS GHA Portal. New accounts can be created by the NPI Administrator or by the User through the registration process. All new User access must be approved by an NPI Administrator.

**User Administration**
Please use this tool to find users that have access to the Service Locations (NPIs) that you administer, or to add a new user to one or more of the Service Locations (NPIs) that you administer.

Click “User Administration” from the left navigation to begin, then use the drop-down and choose “Find Users” to locate current users or “Add New User” to add a new user for the first time.
ADD NEW USER
As an NPI Administrator, you may want to create new user accounts for employees or contractors without making them go through the registration process themselves.

- Choose “User Administration” from the left navigation, then choose “Add New User.”

- Create a user login ID for the new user.

- Enter billing provider credentials.

- Enter the new user’s personal information. Ensure you have confirmed their identity.
- Grant access to specific NPI Practice Locations, or all of them at once. When finished, click “Save Changes” to complete the process or “Cancel” to end the process without saving. The new user will receive an email with a temporary password to access the portal. They will need to change the password upon first login.

**FIND AND ADMINISTER CURRENT USERS**

Administrators are responsible for the users under their account. This includes updating the user’s account information, resetting passwords as well as secret questions and answers, and removing access when someone no longer needs it.

- Choose “User Administration from the left navigation panel. Use the dropdown to find users that match search criteria, have access to a specific service location, or all users you administer. Then choose “Find Users.” If you choose users that match search criteria or users that have access to a specific service location, you will be presented with a pop-up where you must also enter the criteria and/or choose the service location.
• Once selections have been made, a list of users you administer that fit the criteria will be presented. Click on their User ID to land on the “Edit User” page. From here you can choose “Reset Password,” or “Reset Q&As” to perform those actions. A confirmation pop-up will appear confirming that you want to perform the action. You may also choose “User Service Locations (NPIs)” to see and edit a list of the locations this user has access to.

Account Actions

- Reset Password
- Reset Security Q&As
- User Service Locations (NPIs)

• From the “Edit User” page, you may also edit details of the user’s personal information; for example, if the user had a change in name, work address, phone number, or email. Choose “Save Changes” to complete the edits or “Cancel” to cancel the changes.

Personal Information

User Login ID*: 
Name*: 
Work Address Location Name: 
Work Address Line 1*: 
Work Address Line 2*: 
City*: 
State*: 
Zip Code*: X 
Telephone*: 
Email*: 

Save Changes Cancel

Removing Access for Standard and Eligibility Users

It is the responsibility of the Administrator to make sure that all User accounts are updated when users no longer require access to an NPI. Please follow the below steps to remove location to an NPI, DO NOT disable the account as there may be other NPIs that this user has access to that are not connected you.
- From the Left Navigation select User Administration

- After selecting this, find the specific user to update. You can locate the user by selecting **Find Users**.

- Once the user is located, select **User Service Locations (NPI)**

- Search for the NPI and select **Remove**
My Transactions

Eligibility

Eligibility Check
Accessible by all portal users, this page allows providers to check for eligibility data for the beneficiaries they represent. This section is used to verify, not to determine, Medicare eligibility.

The Portal provides beneficiary eligibility information 24 hours a day, 7 days a week.

- The eligibility data is considered accurate at the time of the request.
- Questions regarding eligibility/benefit date for Medicare Part A and Part B should be directed to the appropriate Medicare Administrative Contractor (MAC).
- Eligibility/benefit questions about Medicare Advantage (MA) and Medicare Secondary Payer (MSP) needs to be directed to the appropriate plan.
- Eligibility/benefit questions concerning Qualified Medicare Beneficiary (QMB) eligibility needs to be directed to the State online Medicaid eligibility system. Also reference Medicaid Identification cards and documents issued by the state proving QMB eligibility.
- To perform an Eligibility search, follow the below steps:
  - Select “Eligibility Check” from the left side navigation bar of the account dashboard.
  - Choose the NPI Service Location (and region, if applicable)
    - Enter Patient’s Medicare Number
    - First Name
    - OR
    - Date of Birth
    - AND one of the following
      - Last Name
      - Suffix (if applicable)
      - Date of Service (optional)
  - To submit the request, select “Check Eligibility.” If you would like to start over, select “Clear Form.”
If any element is not correct, users will receive an error message in red at the top of the page explaining which element is incorrect.

- Invalid First or Last Name. Please correct and re-submit. (CICS 3002)

If all elements are correct, users will be presented with the Eligibility Summary page that offers high-level eligibility information. Additional details are displayed in boxed categories located at the top of the page. If additional information is available the category box will be blue, if no additional information is available, the category box will be grey. Category box order will vary depending on availability.

If you need to print this information, click on the blue Print button, it will print a summary of the information for all eligibility tabs at one time.
Eligibility Viewer
Eligibility Check Actions

The WPS GHA Portal utilizes the HIPAA Eligibility Transaction System (HETS), as required by CMS, as the authoritative source for all eligibility inquiries. Although the data from HETS is real-time, the data available in the HETS 201/21 system comes from many different sources that may take up to two weeks to update. As soon as data is available in the HETS 201/21 system, users of the portal are able to view it. View more information about HETS on the CMS website.

(Note: available real-time information will be displayed under the highlighted tabs.)

Patient Eligibility Summary

The eligibility data included is considered accurate at the time of the request.

Questions regarding eligibility/benefit data for Medicare Part A and Part B should be directed to the appropriate Medicare Administrative Contractor (MAC).

Part A Entitlement

<table>
<thead>
<tr>
<th>Part A Entitlement</th>
<th>Base</th>
<th>Remaining</th>
<th>Amount</th>
<th>Effective Date</th>
<th>Termination Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lifetime Reserve</td>
<td>50</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lifetime Reserve Days</td>
<td>60</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lifetime Reserve Copayment</td>
<td>$502.00</td>
<td>01/01/2019</td>
<td>12/31/2019</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AVAILABLE ELIGIBILITY INFORMATION

- Summary
  - Date of Death
  - Part A/B Entitlement Dates
  - Previous Part A/B Entitlement Date
  - Yearly Part A/B Benefit Information
  - Part A/B Ineligible Dates
  - Part A Lifetime Reserve Days
  - Part A Lifetime Reserve Co-Payment Amount
  - Part A Lifetime Psychiatric Days
  - Part A Hospital Days
  - Part A Hospital Co-Payment Day and Amount
  - Part A Skilled Nursing Facility (SNF) Days
  - Part A Skilled Nursing Facility (SNF) Co-Payment Days and Amount
  - Part B Pulmonary Rehabilitation Sessions
  - Part B Cardiac Rehabilitation Sessions
  - Part B Intensive Cardiac Rehabilitation Sessions
  - Blood Deductibles
  - Smoking Cessation (Base Sessions, Remaining Sessions and Date of Initial Cessation with 12 months (if applicable))
- **Part A Deductible**
  - Part A Individual Hospital Spell Dates and Co-Payments, Deductible Remaining
  - Part A SNF Individual Spell Dates and Co-Payments, Deductible Remaining

- **Part B Deductible**
  - Coverage Year
  - Deductible Base
  - Deductible Remaining

- **Medicare Secondary Payer (MSP)**
  - Enrollment and Termination Dates
  - Type Code and Description
  - Name
  - Address
  - MSP diagnosis codes related to each MSP enrollment period

- **Preventative Service Information**
  - Procedure Code
  - Professional/Technical Modifier
  - Next Eligible Date

Preventive services information displays current information only. No inference about historical eligibility can be made based on the returned next eligible dates. The next eligible date is the date on which the Medicare Beneficiary is/was eligible to receive services specified by the Health Care Procedure Coding System (HCPCS) based on the HETS 270/271 application.

If the technical and professional components of a HCPCS code have different next eligible dates, then the HETS 270/271 application will return separate dates for each.

- Annual Depression Screening includes code G0444.
- Annual Wellness Visit (AWV) includes codes G0438 and G0439.
- Cardiovascular Disease Screening (CARD) includes codes 80061, 82465, 83718, and 84478.
- Colorectal Cancer Screening (COLO) includes codes G0104, G0105, G0106, G0120 and G0121.
- Computed Tomography Bone Mineral Density Study includes code 77078.
- Diabetes Screening Tests (DIAB) includes codes 82947, 82950, and 82951.
- Dual Energy X-ray Absorptiometry (DXA) Bone Density Study; axial skeleton includes code 77080.
- DXA Bone Density Study; appendicular skeleton includes code 77081.
- Fecal Occult Blood Test (FOBT) includes codes G0328 and 82270.
- Glaucoma Screening (GLAU) includes codes G0117 and G0118.
- Intensive Behavioral Counseling for Obesity includes code G0447.
- Intensive Behavioral Therapy (IBT) for Cardiovascular Disease (CVD) includes code G0446.
- Initial Preventive Physical Examination (IPPE) includes codes G0402, G0403, G0404, and G0405.
- Pneumococcal Vaccine (PPV) includes codes 90669, 90670 and 90732.
- Prostate Cancer Screening (PROS) includes codes G0102 and G0103.
- Screening and High Intensive Behavioral Counseling (HIBC) to prevent STIs includes code G0445.
- Screening Mammography (MAMM) includes codes G0202 and 77057.
- Screening Pap Test (PAPT) includes codes Q0091, P3000, G0123, G0143, G0144, G0145, G0147, and G0148.
- Screening Pelvic Exam (PCBE) includes code G0101.
- Single Energy X-ray Study includes code G0130.
- Ultrasound Bone Density Measurement and Interpretation includes code 76977.
- Ultrasound Screening for Abdominal Aortic Aneurysm (AAA) includes code 76706 (effective 01/01/2017).
- Hepatitis B Screening includes code G0499 (effective 04/06/2019).

**Prescription Drug Plan (PDP) Information**
- Enrollment and Termination Dates
- Contract and Plan
- Name
- Address
- Telephone Number
- Web Address (if available)

**Therapy Cap Information**
- Occupational Therapy Cap
- Year
- Dollar Amount Used
- Physical/Speech Therapy Cap
- Year
- Dollar Amount Used

- Managed Care Organization (MCO/HMO) Information (also known as “Medicare Part C” or “Medicare Advantage”)
  - Enrollment and Termination Dates
  - Contract and Plan
  - Name
  - Address
  - Telephone Number
  - Web Address (if available)
  - Enrollment Plan Type
  - Bill Option Code
  - MCO and PBP information will be displayed on separate lines

- End Stage Renal Disease (ESRD) Information
  - ESRD Coverage Period Effective Date
  - ESRD Coverage Period End Date (if applicable)
  - ESRD Dialysis Start Date (if applicable)
  - ESRD Dialysis End Date (if applicable)
  - ESRD Transplant Date (if applicable)

- Home Health Information
  - Home Health Periods Start and End Dates
  - Date of Earliest and Latest Billing
  - Provider NPI
  - Contractor Number and Name
• Hospice Information
  o Hospice Provider ID
  o Hospice Start and End Dates
  o Hospice Revocation Code

• QMB Information
  o QMB Enrollment Period

A Qualified Medicare Beneficiary (QMB) is eligible for both Medicare and Medicaid. Medicare providers and suppliers may not bill people in the QMB program for Medicare deductibles, coinsurance, or copays, but state Medicaid programs may pay for those costs. Under some circumstances, federal law lets states limit how much they pay providers for Medicare cost-sharing. Even when that’s the case, people in the QMB program have no legal obligation to pay Medicare providers for Medicare Part A or Part B cost-sharing. Look at the patient’s Medicare, Medicaid or QMB card to see if the patient is enrolled in a QBM.

• MDPP Information
  o MDPP Effective Date
  o MDPP Termination Date
  o Inactive Coverage
  o Active Coverage
  o Additional MDPP HCPCS codes with actual usage
  o Billing Provider NPI
  o Date of Service for each HCPCS code
  o MDPP Period 2 End Date

Medicare Diabetes Prevention Program (MDPP) a structured intervention with the goal of preventing type 2 diabetes in individuals with an indication of pre-diabetes. This program is available for a minimum of 12 months and a maximum of 24 months. The maximum period is determined by the MDPP Period 2 End Date.

The MDPP tab displays when a beneficiary is enrolled in MDPP within the date of service range you requested on your eligibility search. If you are an MDPP provider, only limited eligibility containing the Part B eligibility date on the Summary page, the MCO, MSP and ESRD tabs will display any data (if applicable). Please note: The Effective Date for Active Coverage only displays the starting date of service that was submitted on the eligibility request. It is NOT the actual start date for the beneficiary’s MDPP. If the beneficiary’s MDPP enrollment is not active, it will display the starting date of service that was submitted on the eligibility request on the Inactive Coverage line.
Medicare Beneficiary Identifier (MBI)

MEDICARE BENEFICIARY IDENTIFIER (MBI) LOOKUP
This tool is to be used only when a Medicare patient doesn’t or can’t give you his/her Medicare Beneficiary Identifier (MBI). The patient’s first name, last name, date of birth, and social security number are required to get a unique match. The MBI is confidential so you’ll have to protect it as Personally Identifiable Information and use it only for Medicare-related business.

- On the MBI Lookup Search page, select the dropdown arrow for the Service Location (NPI).
- Find and select your NPI and click Continue. If you have a single NPI, the program will default the selection.
- Enter the patient’s Social Security Number (SSN)
- Enter the patient’s First Name
- Enter the patient’s Last Name
- Enter the patient’s Suffix (if there is one)
- Enter the patient’s date of birth and Click Submit

Possible messages that you will see in this search feature:
- If the patient is deceased and has been for more than 13 months in the past, you will see “Date of Death xx/xx/xxxx exceeds timely claim filing requirement.

If an MBI is found with the information submitted, you will be taken to the MBI Results page with the patient’s new MBI. You can perform additional actions on this page:
• Click on the Search button. This will take you back to the MBI Lookup Search page with all previous entered data still populated in the fields.
• Click on the New Lookup button. This will take you back to the MBI Lookup Search page with all previous data cleared from the fields.
• Click Check Eligibility and this will take you to the patient’s Eligibility Summary page for the current date. (For further eligibility information please see that section of the manual).
• Print the MBI Results page by clicking the Print button.

---

Claims (Part B Paper Claims Submitters Only)

REGISTER FOR ONLINE CLAIM ENTRY

• On the “My Dashboard” homepage select “Claims” from the left-hand navigation bar.
• On the Claims page select the “Claim Entry Registration” button.
• The Claim Entry Registration page will open in a new tab, containing instructions on how to complete the EDI self-service registration will open.
  o Make sure to read all of the instructions on the form. Submitter ID, Submitter name field and selecting “5010 837 Professional Claim Inbound” on the registration page is critical.
  o Click on the “Register here for online claim submission” link.
• A tab will open loading the Provider EDI Self-Registration page. Enter your email address and select “Medicare” as your division. Then finish entering the rest of the information on this page as required and remember to follow the instructions Complete the information on this page, selecting “Medicare” as your Division and remembering the special instructions in the “Claim Entry Registration” tab.
• The EDI department will be in touch with you via email to obtain your WPS GHA Portal User ID, so they can update your account for claim entry submission.

NOTE: Please allow up to 30 calendar days for the EDI Department to receive, review and
setup the NPI you listed for claim entry with your account.

**NOTE:** If at any time your Portal User Login ID ever becomes disabled and you registered for a new Portal User Login ID, you will need to re-enroll any NPIs again for online claim entry as described above so that you will again be able to submit claims online.

**Submit New Claim**

**NOTE:** Please note that currently the Claim Entry functionality does not accept Medigap, MSP, Hospice (place of service 34), or Purchased Service claims. Any fields denoted with an asterisk (*) are required fields. All others are optional.

- On the “My Dashboard” Homepage select “Claims” from the left-hand navigation bar.
- On the Claims page select the “Submit New Claim” button
Select the NPI Service Location from the list that the claim will be filed under.
Enter the Federal Tax ID Number (if the provider bills under Social Security Number, enter SSN).
Select the appropriate bullet (SSN or EIN).

Enter the Patient’s Medicare Number as shown on the patient’s Medicare card.
Enter the patient’s name exactly as shown on the patient’s Medicare card. First Name, Middle Initial (if any), and Last name.
Enter the patient’s 8-digit Birth Date.
Select the bullet to the left of the correct gender for the patient.
Enter the patient’s full mailing address including street information, City, State, and ZIP Code.
- Accept Assignment - Select the bullet to the left of the correct assignment to indicate whether or not the Provider accepts assignment.
- If you know the specific specialty you are billing for, select “I am billing charges for” from the expanded drop-down list. If none apply, select “None of the following apply to my claim.”

- Hospitalization Date - If billing a Place of Service (21, 51, or 61 only) enter the current service Admission and Discharge dates.
- Service Facility Location:
  - Enter Location Name
  - NPI (if available)
  - Address of facility where services were performed.
- Referring Provider or Other Source Name:
  - Enter the Name of the referring or ordering physician if the service or item was ordered or referred by a physician.
  - When a claim involves multiple referring and/or ordering physicians, a separate claim form shall be used for each ordering/referring physician.
  - Enter the NPI of the referring/ordering physician listed in the Referring Provider or Other Source Name field. All Physicians who order services or refer Medicare beneficiaries must report this data.
- Enter any necessary narrative comment, you may include up to 80 characters maximum.
- Enter the Investigation Device Exception # when an investigational device is used in an FDA approved clinical trial.
- Patient’s Account # - Enter the patient’s account number assigned by the provider of service or supplier accounting system.
- Patient Paid Amount $ - Enter the total amount the patient paid towards this claim on the covered services only.
**Diagnosis or Nature of Illness or Injury:**
- Select the bullet to the left of the ICD version that applies 9 or 10.
- In field 1, enter the primary diagnosis code that applies to the claim.
- Any additional diagnosis codes for this claim should be entered in the additional 2-12 fields in priority order of importance.
  - **Do not enter any decimal points.**

**Number of Lines:**
- Select the number of lines from the dropdown box.

**Date of Service:**
- Enter from date and to date(s) of service for the first line item.

**Procedure:**
Enter the 5-digit procedure (HCPCS or CPT) code for this line item.
When reporting an “unlisted procedure code” or a “Not Otherwise Classified” (NOC) code, the NOC Description field is required.

- **Place of Service:**
  - Enter the 2-digit Place of Service code.

- **Modifier:**
  - Enter any applicable 2-character procedure code modifier in field 1.
  - Any additional applicable modifiers should be entered in field 2, then 3, then 4.

- **Diagnosis Pointer:**
  - This is a “Diagnosis Pointer” field that corresponds to the previous Diagnosis section.
  - Enter “1” if the first diagnosis code you entered is the main diagnosis for this line item.
  - Enter “2” if the second diagnosis code you entered is the main diagnosis for this line item, etc.
  - Do not enter 01, 02, 03, etc.

- **Charges:**
  - Enter the dollar amount you are billing for this line item.

- **Is this anesthesia?**
  - Check the bullet to the left of “Yes” if this is an anesthesia service.
  - Check the bullet to the left of “No” if this is not an anesthesia service.

- **Units:**
  - (If “No” was selected for “Is this anesthesia” question)
  - Enter the number of “units” or “like services” for this line item.
    - Units cannot be zero.

- **Minutes:**
  - (If “Yes” was selected for “Is this anesthesia” question)
  - Enter the total number of minutes for that line item.
    - Minutes cannot be zero.

- **Rendering Provider:**
  - Enter the First Name, Last Name, and NPI of the provider that performed the service, if different from the billing provider.

- **NOC Description:**
  - If you reported an “unlisted procedure code” or a “not otherwise classified” (NOC) code as the procedure, you will need to enter the description of service into this field.
    - It can be up to 80 characters.

If you have additional service lines to enter and you did not select from the Number of Lines dropdown box, select in the “Add new line” button.
- This will expand the screen to include “Claim Line 2” information to be entered.
- You will be able to enter up to 12 claim service lines.
- If you selected to add additional lines but need to delete one, a red “Delete Line” button will appear on every line starting at line 2.
Claim Lines [Max 12] [CMS 1500. Box 24]

Line: 1

Date of service*: From: mm/dd/yyyy  To: mm/dd/yyyy

Procedure*: CPT/HCPCS*: Place of Service*

Modifier:

Diagnosis Pointer*:

Charges $*: 0.00

Is this anesthesia?  Yes  No

Units*: 1

Rendering Provider: First Name  Last Name

NPI

NOC Description: 80 Characters maximum

Add new line

Line: 2

Want to copy information from another line?  Line:
When all claim lines have been entered, select “Review.”
  o “Edit” and “Submit” buttons will now appear.
If errors exist a message will display at the top of the Claims page indicating what needs to be corrected. You will need to correct the errors prior to submitting the claim.
  o If you find errors, select “Edit” to make changes.
  o If you are satisfied the claim is entered correctly select “Submit”
If no errors are presented review your claim.
If you selected “Submit” a message will display at the top of the New Claim screen with a confirmation number.
Once completed you have the option to print a copy of the confirmation screen by selecting “Print.”
To begin entering another claim select “Start New Claim” to be taken back to a blank Claim Entry Screen.
  o It is recommended that you print this confirmation page for your records.
  o If for any reason a claim is rejected from the Medicare front end system, the receipt number will be referenced in the educational contact to you.
SPECIALTY CLAIMS FIELDS

Ambulance Services

*Pick up Location Address:* Enter the No., Street, City, State and Zip Code at the location the patient was picked up.

*Drop-off Location Name:* Enter the Name of the facility at the location the patient was dropped off.

*Address:* Enter the No., Street, City, State and Zip Code at the location the patient was dropped off.

*Reason for Transport:* Select the bullet left to the appropriate reason for the transport. Only one may be chosen. When selecting the reason for transport, you must also include the Transport Distance in Miles field.

*Purpose of Round Trip:* Free form description explaining the reason for round trip.

*Stretcher Purpose Description:* Free form description explaining the purpose of stretcher.

*Transport Distance in Miles:* Enter the distance of the transport in miles. When entering information in this field, you must also select the reason for transport.

*Condition of Patient:* Select the bullet left to the appropriate condition of patient. You may select more than one condition.
Chiropractic Services

*Initial Treatment Date:* Enter the Initial Treatment Date (initiation of the course of treatment).

Global Surgery Services

*Assumed Care Date:* Enter the assumed care date for global surgery when providers share post-operative care.

*Relinquished Care Date:* Enter the relinquished care date for global surgery when providers share post-operative care.

Inpatient Services

*Admit Date:* Enter the date the patient was admitted.

*Discharge Date:* Enter the date the patient was discharged if known.

Laboratory Services

*CLIA#:* Enter the 10-digit Clinical Laboratory Improvement Act (CLIA) certification number for laboratory services billed by an entity performing CLIA covered procedures.

*Referring CLIA#:* Required for any laboratory that referred tests to another laboratory covered by the CLIA Act that is billed. Enter the 10-digit CLIA certification number for the referral laboratory.
Occupational/Physical Therapy Services

*Date Last Seen:* Enter the Date Last Seen by the supervising provider.

*Supervising Physician Name:* Enter the First Name and Last Name of the patient’s attending physician.

*Supervising Physician NPI:* Enter the NPI of the patient’s attending physician.

**NOTE:** Name and NPI are optional. If you enter one of these three fields, you must enter all three.

Mammography Services

Mammography Certification #: Enter the 6-digit FDA approved Mammography Certification number.

Routine Foot Care

*Date Last Seen:* Enter the date the patient was last seen by their attending physician.

*Supervising Physician Name:* Enter the First Name and Last Name of the patient’s attending physician.

*Supervising Physician NPI:* Enter the NPI of the patient’s attending physician.

Claim Inquiry

**CLAIM STATUS - PART A AND PART B**

- Choose the “Claim Inquiry” link on the left-hand navigation panel.
- Choose the NPI Service Location (and region, if applicable) that you are requesting claim status for from the dropdown.
- Enter the following:
  - Patient’s Medicare Number
  - First Initial
- Select “Search”

- If a claim is on file for the information you entered, you will be brought to the Claim Results page, which gives high level claim information. Scroll to the bottom of the page and select the link under the “Claim Number” to obtain claim details. Alternatively, and if applicable, you can begin the process of submitting medical documentation (MR), a reopening (CER) or an overpayment (OCA), by clicking the appropriate box under the “Actions” heading.

Claim Results

2 Claims found.
Note: not all claim actions are available for all claims.

<table>
<thead>
<tr>
<th>Region</th>
<th>Claim Number</th>
<th>Date</th>
<th>Amount Billed</th>
<th>Process/Finalized Date</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>JSB</td>
<td>717199075000</td>
<td>mm/dd/yyyy</td>
<td>Amount ($)</td>
<td>mm/dd/yyyy</td>
<td>Status</td>
<td>Actions</td>
</tr>
<tr>
<td>JSB</td>
<td>717199075010</td>
<td>mm/dd/yyyy</td>
<td>Amount ($)</td>
<td>mm/dd/yyyy</td>
<td>Status</td>
<td>Actions</td>
</tr>
</tbody>
</table>

- To return to the main Claims screen select “Refine Search” (this will retain all previously
entered data) or select “New Search” (this will clear the form and you can begin a new claim status search).

- If no claims are on file based on the information provided the message “No claims found for search criteria in (region selected)” will appear at the top of the screen.

- If a Part A claim has been archived, you must call the Provider Contact Center (the appropriate number to call will be displayed).

CLAIM DETAILS
The claim details page provides a more in-depth view of how a claim processed. If there are underlined lines similar to links, you may hover or click on them with your mouse to show more information.

The following information can be found on this page, if applicable:

- Status (i.e. Adjusted/Replaced, Processed, Finalized/Paid, In Process, Denied, Cancelled)
- Date Received
- Processed Date
- Check/Electronic Funds Transfer (EFT) Number
- Check Date
- Allowed Amount
- Payment Amount
- American National Standards Institute (ANSI) Group Codes
- Claim Adjustment Reason Codes
- Remittance Advice Remark Codes
- Remittance Advice (RA Date)
- Pay Codes
- Rendering NPI
- Rendering Provider name
- Claim line details
- Document Control Number (DCN)
- Type of Bill
- Status/Location
- Remark Codes
- Reason Codes
- Discharge Status
- Blood Deductible

After you are finished viewing the claim details you can select the “Back to Claims Results” link to return to the previous Claim Results page.
In the Claim Details table, information under the grey bar on the left half of the section includes information received from the provider. The information on the right half of the section under the blue bar, is information generated by WPS GHA and reflects information included on the remittance advice, as well as a More Info button.
Information available under the More Info button (If applicable to the claim line):

- Rendering Provider
- Rendering NPI
- ANSI Reason and Remarks codes
- Related Claim Link – Provides a link to a claim that may be duplicative of your claim.
- Patient Eligibility Information
Enhanced denial information is available for some denials. It will provide the information available for all claim lines with a More Info button, and will also include if available:

- Additional information explaining the denial reason
- Tips and suggestions if you believe the claim was not submitted correctly
- Links to other web pages or web sites if additional information is available

Claim actions such as Resubmit Claim (New) or Reopen (Clerical Error) if appropriate (Claim actions may not be available for all denials)

For claims denied due to a policy, if the enhanced denial information is available, there will be a link to the policy housed at the CMS website.
For claims denied because of an eligibility issue (MSP, MCO/HMO, Hospice, etc.), where enhanced denial information is available, eligibility can be verified from the enhanced denial script.

CLAIM ACTIONS
On the “Claim Details” page, there is a section of buttons or links of available actions you can take on a claim. Not all actions will be available on every claim. These actions include:

- “Add Documentation” (Medical Documentation for ADR requests)
- “Download Remit” (to obtain remittance)
- “Reopen Clerical Error” (to perform a reopening)
- “Report Overpayment” (Overpayments)
- “Request Redetermination” (Appeal)
- “Check Patient’s Eligibility” (Eligibility)

Click the applicable button to start the process. See the specific manual section for details and step by step instructions on each of these items.
Clerical Error Reopening (CER)

SUBMITTING A CLERICAL ERROR REOPENING (CER)
Clerical Error Reopen (CER) submission enables Providers to enter revised claim information that will be transmitted through the WPS GHA Portal to the Multi-Carrier System (MCS). The CER feature will allow for changes to specific claim information on a denied claim and immediate notification that the claim adjustment has been accepted into MCS.

There is not a claim line limit and if you have one or more of the following situations, request a CER through the Portal. If the situation does not fall under one of these options a redetermination will need to be submitted:

- Change Rendering Provider National Provider Identifier (NPI)
- Add/Change/Delete Diagnosis Code(s)
- Change Date(s) of Service (DOS)
- Change Procedure Code
- Add/Change/Delete Claim Modifier(s)
- Change Billed Amount – Related to Fee Schedule Change
- Change Billed Amount – NOT Related to Fee Schedule Change
- Change Units of Service Billed

There are a few limits to the above changes. If you need to change the billed amount, you cannot also change the number of services. Likewise, if you change the number of services, you cannot also change the billed amount. **Claims can only be adjusted once via the Portal, so make sure you update all applicable fields before submitting the CER.** For example, if a date of service change is submitted through the Portal, you cannot adjust the claim a second time in the Portal when the claim finalizes.

To submit a CER please follow the below steps:

- From the “My Dashboard” homepage select the link for “Claim Inquiry.”
- Follow the below steps in the “Claim Status Part A and Part B” instructions to get to the claim details page.
- On the claim details page, under “Claim Actions,” if your claim is eligible for a reopening the “Reopen (Clerical Error)” button will be in dark blue. Select “Reopen (Clerical Error)” to proceed.

Claim Actions

- Add Documentation
- No Remit Available
- Reopen (Clerical Error)
- Report Overpayment
- Request Redetermination
- Check Patient’s Eligibility

- On the Edit Claim - Clerical Error Reopening screen all fields are editable.
Make all needed changes to the claim. If the billed amount is changed, an additional question of whether that change was a “Fee Schedule Change” or not must be
completed (Yes or No selected in a dropdown box) prior to being able to complete the claim adjustment. Once all changes have been made, click on the “Review” button.

- The Edit Claim – Clerical Error Reopening screen will display a message stating “Your information has been successfully reviewed, to finalize your adjustment request, click the Submit button.”
  - To finalize select “Submit”
  - To edit your former entry, select “Edit” to make changes and select “Review” again.
  - To cancel the request entirely select the “Cancel” button, this will return you to the Claims page.

- On the Clerical Error Reopening Confirmation screen, please take note of the new Claim Number which you will need to search for claim status or to use the Appeal Status feature. This Confirmation page containing your new Claim Number can be printed for your records by selecting “Print.”

![Clerical Error Reopening Confirmation](image)

**COMMON ERROR MESSAGES AND THEIR CAUSES**

- Claim processed more than 1 year ago. Reopening not allowed unless good cause can be established. Please see IOM 100-4 Chapter 34 Section 10.11 to determine if good cause exists. If so, submit request in writing with good cause documentation.
  - **Cause:** Initial claim processed more than one year ago.

- Claim has been previously adjusted, please submit a redetermination request.
  - **Cause:** Claim has been previously adjusted.

- Procedure code not valid or Place of Service not valid for Procedure code - reopening not allowed for this change.
  - **Cause:** The place of service does not match the procedure code billed, or the procedure code is not valid. Since the information would cause the claim to deny again, a reopening cannot be completed.

- Due to complex nature of the requested change this request cannot be handled as a reopening. Please submit redetermination request.
  - **Cause:** The claim you are trying to adjust contains modifiers: 22, 23, 53, 55 62, 66, 74 or CR. In these situations, we must review additional documentation to process the claim. For this reason, the request is too complex, and you will need to resubmit a redetermination request with the
Requested diagnosis code is invalid, please recheck diagnosis code. No reopening allowed for invalid diagnosis code.
  - **Cause:** An invalid diagnosis code will cause the adjustment to deny.

Due to the complex nature of this claim, you must submit a redetermination request.
  - **Cause:** The claim is for a CPT procedure code ending with a “99.” These codes are generally “not otherwise classified.” A claim determination for these procedure codes requires medical review of documentation. This cannot be done as a reopening since we must review the medical documentation to determine coverage and payment.

Claim cannot be reopened because there is no initial determination for this claim. Please submit a new corrected claim or wait until the claim in process has finalized.
  - **Cause:** The initial claim denied with no appeal rights (unprocessable denial) or a claim is still in pending status. If the claim denied with the MA-130 message, you need to submit a corrected claim. You can use the claim status feature to determine if there is a claim pending which is preventing you from requesting a reopening.

Cannot start with “J”
  - **Cause:** The procedure codes that start with a “J” frequently require special pricing guidance and would be considered too complex to be completed online. These types of claims must be submitted in writing or as an appeal request. You can either file a Redetermination in the portal or a paper Reopening. Note: this is even if you are not trying to adjust the ‘J’ code.

**Overpayments (OCA)**

**OVERPAYMENT CLAIM ADJUSTMENTS (OCA)**
Medicare Part B providers can submit Medicare Secondary Payer (MSP) and Non-MSP overpayment adjustments via the Portal. Please follow the below steps:

- Follow steps 1 – 6 in the “Claim Status Part A and Part B” instructions.
- On the claims page under “Claim Actions” if your claim is eligible for an overpayment request the “$ Report Overpayment” button will be in dark blue. Select “$ Report Overpayment” to proceed.
  - You may also select the “OCA” button under Actions.
An Overpayment Claim Adjustment box will display. Select the Non-MSP or the MSP reason for the overpayment from the dropdown box.

- Based on your selection additional applicable fields will display. For this example,
Services not Rendered was selected.
- To proceed with the request, check the “Deny This Claim Line” check box
- Select “Review”
- To cancel your request, select “Cancel” to be taken back the Claim Details.

- A message will display on the page indicating to select “Submit” to finalize the adjustment request. Select “Submit” if you are ready to finalize the overpayment request.
- An Overpayment Claim Confirmation screen will display providing you with your new Claim Number. You can print this page for your records.

**NOTE:** Before an adjustment for HMO/MCO, SNF, Home Health, Hospice, and all of the MSP can be completed, the Portal will check Medicare’s files for a valid matching record.

**Medical Documentation**
- Choose the “Medical Documentation” link from the left navigation pane.
  - Choose “Search Documentation” to search for previously uploaded medical documentation. See the “Search Documentation” instructions below.
  - Choose the “Prepayment Review” tab to upload medical documentation for claims that have an Additional Documentation Required (ADR) status. See the “Prepayment Review Tab” instructions below.
  - Choose the “Post-payment Review” tab to respond to a probe. See the “Post-payment Review Tab” instructions below.
There is also an option to submit an ADR response through Claims Inquiry. This is the most accurate method. See the “ADR Response using Claim Inquiry” instructions below.

**SEARCH DOCUMENTATION**

- After choosing “Medical Documentation” from the left navigation pane, choose “Search Documentation.” If there is documentation available, the medical documentation search results page will load with a list.
  - Use the “My Submissions Only” button to show only documents you have submitted.
  - Use the “Show entries” dropdown to increase the results per page.
  - Sort using the arrows next to the headings.
  - Filter using the “Filter” box.
  - Use the page buttons at the bottom to move between pages.
  - Click on a confirmation number link to pull up that specific documentation information.
After clicking on the confirmation number link, the Medical Documentation Detail page will load. This pop-up will include the details of the documentation, as well as links to the files themselves.

- Use the “Show entries” dropdown to increase the results per page.
- Use the “Filter” box to filter the results.
- Click on the file name link to open the specific document.
- Use the “Print” button to print the document for your records or the “Ok” button to return to the search results page.
ADR RESPONSE

- After choosing “Medical Documentation” from the left navigation pane, choose the “Prepayment Review” tab. Select the NPI Service Location (and region, if applicable), enter the Provider Number (PTAN), Patient’s Medicare Number, Claim Number, and the Start and End Date of Service. Choose a file to upload with the “Browse” button. Choose “Submit” to move to the next step, or “Clear Form” to start over.

- After successfully submitting, you will be brought to the Medical Documentation Detail page. This page will include:
  o Submission information section, which will include a confirmation number.
  o Information provided section, which will include provided details.
  o Attached documentation section, which will include any submitted documentation.
  o Use the “Show entries” dropdown to show additional entries per page.
  o Use the “Filter” box to filter results.
  o Use the “Print” button to print for your records, select “Ok” to finish and return to the previous screen.
ADR RESPONSE USING CLAIM INQUIRY

- The most accurate way to submit an ADR response is using the "Claim Inquiry" option. After choosing "Medical Documentation" from the left navigation, from the ADR Response tab, choose the "Claims Inquiry" link located in the paragraph below the ADR Response/Probe Response tabs, or simply click the "Claim Inquiry" link from the left navigation.
- Find the claim in question. See “Claim Inquiry” instructions for full instructions on claim inquiry.
- Choose the appropriate claim by choosing the claim number link from the claim results to get to the claim details page.
- On the details page under “Claim Actions,” look for the “Add Documentation” button. If an ADR was requested/available, it will be clickable and darker blue. If it is not available/an ADR was not requested, it will not be clickable and lighter blue.

**Claim Actions**

- A pop-up will appear allowing you to add the necessary files. Choose “Browse” to add the file, then choose “Review” to continue, or “Cancel” to end the process.
The confirmation pop-up box will appear where you can review the information for accuracy and completeness. Choose “Submit” to finalize, “Edit” to make changes, or “Cancel” to end the process.

A final submission confirmation will pop-up with an informational message and a confirmation number. Take note of the confirmation number or print for your records using the “Print” button. Use the “Close button when finished to return to the claim detail page.
**POST-PAYMENT REVIEW TAB**

- After choosing “Medical Documentation” from the left navigation pane, choose the “Post-payment Review” tab. Choose the NPI Service Location (and region, if applicable), enter the Provider Number (PTAN), Probe Number, Patient’s Medicare Number, Claim Number (ICN/DCN), and the Start and End Date of Service. Choose a file to upload with the “Browse” button. Choose “Save and Submit another File” if there is another file to submit for the same probe. Choose “Submit and Finish” once all claim numbers for the probe have been completed. Choose “Clear Form” to clear the current form.

- After successfully submitting, you will be brought to the Medical Documentation Detail page. This page will include:
  - Submission information section, which will include a confirmation number.
  - Information provided section, including provided details such as probe number.
  - Attached documentation section, which will include any submitted documentation.
  - Use the “Show entries” dropdown to show additional entries per page.
  - Use the “Filter” box to filter results.
  - Use the “Print” button to print for your records, select “Ok” to finish and return to the previous screen.
Remittance Advice

There are two ways to obtain a duplicate remittance using the portal:

- To access a full remittance, use the “Remittance Search” option from the left navigation panel; follow the “How to obtain a full duplicate remittance from Remittance Search” instructions below.
- To retrieve a remittance from a specific claim, use the “Claim Inquiry” option from the left navigation panel; follow the “Obtain Remittance from Claim Search” instructions below.
NOTE: The remittance obtained will be a full remittance, regardless of how it is accessed.

OBTAIN A FULL DUPLICATE REMITTANCE FROM REMITTANCE SEARCH

- Choose “Remittance Advice” from the left navigation panel. Choose the NPI service location (and region, if applicable).
  - Duplicates are available up to 13 months from the remittance advice date.
  - Remittance notices larger than 150 pages may not be available to view. If you wish to refine your search criteria, use the “Back to Remit Search” link on the top of the Remittance Advice Search page.
  - Incentive/bonus pay remittances are unavailable through the portal.

Remittance Advice Search

Duplicates of Remittance Advises are available up to 13 months from the remittance advice date. Please complete the information below to submit the remittance search.

If you have clicked on View Remit and the remittance advice does not open, please make sure your browser is allowing pop-ups from www.wpsgha.com.

Required fields are marked with an asterisk (*).

Service Location (NPI) #: Select an NPI

Please enter one of the following search criteria groups.

[] Remits for the last 30 days

Remittance Advice Date: mm/dd/yyyy

Remittance Advice Date Range: From: mm/dd/yyyy To: mm/dd/yyyy

Remittance Number (Part A): Remittance Number:

Check / EFT Number: Check / EFT Number

ICN / DCN: ICN / DCN

OR Beneficiary’s Information (all the following fields are required for this criteria)*

Patient’s Medicare Number: Patient’s Medicare Number

Name*: First Name Last Name

Date of Service*: Start: mm/dd/yyyy End: mm/dd/yyyy
There are multiple ways to search for a duplicate remittance:

- To obtain all remittances from the last 30 days, use the checkbox at the top of the criteria groups.
- You can also search using remittance date or date range, remittance number (Part A only), check/EFT number, or ICN/DCN.
- Lastly you can search by patient information.
- Once criteria are entered, select “Search Remittances” to perform search or “Clear Form” to clear all data and start over.

The remittance results, if any, will be displayed. Information such as region, check/EFT #, amount, advice number (if applicable), advice date, and actions will be shown.

- Choose “Refine Search” to refine the current search or “New Search” to start a new search.
- Use the “Show entries” dropdown to expand the number of entries viewable onscreen.
- Use the “Filter” box to filter results.
The arrows next to the headings can be used to sort the fields.

Choose the “View Remittance” link to view a copy of the remittance advice.

**Note:** The browser must not block pop-ups for the www.wpsgha.com website, or you may have issues loading the remittance. If that cannot be changed, and you experience issues, right-click on the “View Remit” link and select “Open in New Tab” or “Open in New Browser.”

### Obtain Remittance from Claim Search

- Use the claim inquiry link from the left-hand navigation panel to find the claim (See claim status instructions for full instructions on claim inquiry).
- Choose the appropriate claim by choosing the claim number link from the claim results to get to the claim details page.
- On the details page under “Claim Actions,” look for the “Download Remit” or “No Remittance Available” button. If one is available, select it to view the remittance. If one is not available, it will not be clickable and will say “No Remittance Available.”

**Note:** The remittance retrieved will be the full remittance.

### How to Find an Offset

- Follow the above steps to find a duplicate remittance
• Drop the first two digits of the FCN and enter that number in the ICN/DCN field. The WPS GHA portal will display all remits associated to that ICN.

Medicare eRefunds

There are two eRefund options:
• Search for previously submitted eRefunds. See the “Searching for previous eRefunds” instructions below.
• Submit a request to electronically withdraw funds from your account for any balance owed to Medicare. See the “Submitting an Electronic Refund” instructions below.

SEARCHING FOR PREVIOUS EREFUNDS
• Choose “Medicare eRefunds” from the left navigation pane, then choose “Search Entries” near the top. Select the NPI (and region if applicable) and enter the PTAN and Tax ID into the appropriate fields.

Enter at least one of the search criteria items (Date Range, Demand Letter Number,
Accounts Receivable Number, Refund Amount, TCN (Tracking Control Number), or Beneficiary’s information). Choose “Search Entries” to begin search or “Clear Form” to start over.

Please enter at least one of the following search criteria.

Refund Payment Date Range:  
Start: mm/dd/yyyy  
End: mm/dd/yyyy  

OR

Demand Letter Number: Demand Letter Number  

OR

Accounts Receivable Number: Accounts Receivable Number  

OR

Refund Amount: $ Refund Amount  

OR

TCN: TCN  

OR

Beneficiary’s Information (All fields required)

Patient’s Medicare Number:*  
Patient:*  
First Initial:*  
Last Name:*  
Date of Service:* mm/dd/yyyy  
Claim Number:*  

The Search Medicare eRefunds results page will load, showing any results that matched the search. The list will always display the TCN, Refund Date, Refund Amount, and Status. If applicable, it will also display the Demand Letter, AR (Accounts Receivable) Number, Patient First/Last Name, Service Date, Claim Number, and Patient Medicare Number. You can:

- Choose “New Search” to perform a new search, “Refine Search” to refine the current search, or “Submit New Medicare eRefund” to submit a new eRefund.
- Choose “Export to Excel” to export the list to Excel for download.
- Use the “Show entries” dropdown to expand the number of viewable entries onscreen.
- Use the arrows next to the categories to sort.
- Use the “Filter” box to filter.
- Click directly on a TCN number link in the list to see additional details. The Medicare eRefund Details pop-up will display and provide the information about that specific eRefund. Select “Close” to exit the pop-up.
- Use the page numbers or “Next” page button to move between pages.
SUBMITTING AN ELECTRONIC REFUND

- Choose “Medicare eRefunds” from the left navigation panel. Continue with the electronic process by choosing the NPI (and region if applicable), and enter the matching PTAN and Tax ID, then choose “Continue” to go to the next step or “Cancel” to exit the eRefund process.
Fill in the Bank Withdrawal Information with the full routing number, full account number, and refund amount. You must use the same account information that is currently on file with Medicare, from the most recent form CMS-588. To protect your information, the system will lock users out of the eRefund option for 24 hours if 3 incorrect entries are made. Choose “Continue” to go onto the next step, or “Cancel” to exit the eRefund process.

- Indicate whether or not Medicare requested this refund. If yes, continue to step A. If no, continue to step B.
If yes was chosen, indicate if the refund is MSP (Medicare is Secondary Payer) or non-MSP. Next, enter the demand letter number or the accounts receivable number, and/or any additional comments if applicable. Choose “Continue” to move to the Confirmation stage or “Cancel” to exit the eRefund process.

If no was chosen, indicate reason for refund, enter patient and claim data, indicate if the refund is MSP or non-MSP, use the dropdown to give specific MSP and non-MSP reasons, and add any additional comments if applicable. Choose “Continue” to go onto the Confirmation stage or “Cancel” to exit the eRefund process.
If continue was chosen, a pop-up confirmation window will appear. Please review all details for accuracy. Choose “Save” to accept, “Modify” to go back and make changes/additions/deletions, or “Cancel” to exit the eRefund process.
If saved successfully, a confirmation message will appear that includes the Payment TCN and Refund Receipt information and will also include a summary of the refund. Choose the “New eRefund Entry” button to create another eRefund, or the “Print” button to print confirmation for your records.

- Letter Search (ADR and Demand Letters)

**SEARCHING FOR AND RESPONDING TO AN ADR OR DEMAND LETTER**

- To view and respond to an Additional Document Request (ADR) or Demand Letter (DL), select Letter Search in the left navigation pane.
- The NPI will default to the primary one on your account, you may need to select a different NPI to view the letter you are looking for. Select ADR Letter to view and respond to a request for information. You can select a letter date range between 2 weeks and 3 months. ADR letters are available for up to 90 days from the letter date, or until a response is received and the claim has been processed. Demand Letters are available for 90 days after the date of the letter.
- Click the binoculars to view the letter. You can click the Claim Number link to view your claim. Click the Respond icon to submit your additional documentation.
• If you receive an email or dashboard alert that you have an ADR but you cannot find the letter, check the box “Include Pending ADRs without Available Letters. If a letter cannot be viewed, the binoculars will be greyed out. It may take a day or two for a new letter to be available to be viewed in the portal. Certain letters cannot be captured by the portal and will not be viewable, but when you receive the paper letter you can still submit your response via the portal.
To view and respond to a Demand letter, select Demand Letter under Letter Type. You can view and the letter, view the claim(s) if available to the portal, click the Immediate Recoupment icon to electronically fill out and print the Immediate Recoupment form, or click the eRefund icon to automatically send your refund via the portal.
**Appeal Search (Redeterminations)**

**SUBMITTING A PART B REDETERMINATION**

- To submit a redetermination, a specific claim must be used. Use the claim inquiry link from the left-hand navigation panel to find the claim (See claim status instructions for full instructions on claim inquiry).
- After identifying the claim and clicking on the claim number to view the claim details, there will be additional actions listed under “Claim Actions.” Choose “Request Redetermination” to begin the submittal process.

**Claim Actions**

- The “Request Redetermination – File an Appeal” pop-up form appears. The top of the form displays the claim information, to help ensure this is the correct claim.
• You will be required to complete all fields that have an asterisk (*).
  o Please indicate if the request will involve an overpayment.
  o All procedure codes that are on the claim will be listed at the top of the box. Select all procedure codes that apply.
  o Fill in all required and/or applicable fields, including reason(s) for disagreement with determination, reason(s) for filing late, if applicable, and any additional information Medicare should consider.

• Fill in requester's information, including name, relationship to beneficiary, address, and phone number.
If there is evidence, records, or documentation to submit, select the “Yes” radio button, then click the “Browse” button. If there is nothing additional to submit, select the “No” radio button.

The following document types can be uploaded via the WPS GHA Portal: .docx, .xlsx, .pdf, .jpg, .jpeg, .gif, .tif, .tiff, .zip.

- File sizes cannot exceed 15 MB (15,360 KB), and if you are uploading multiple document files for a single request, we require all documents in a single .zip file not to exceed 20 files.

To attach documentation, follow the below steps:

- Click on the Browse button
- In the Choose File to Upload box, find the file to upload
- Highlight document
- Click “Open”
- The Upload box will disappear and the WPS GHA Portal will show the file you selected in the File box

Read the electronic signature agreement and select either the “I Agree” or “I Do Not Accept” radio button. After accepting, select the “Review” button to move on to the review/confirmation stage. By not accepting, the redetermination request will not be able
to be submitted. Otherwise select the “Cancel” button to cancel and return to the claim detail page, or the “Clear” button to clear the form and start over.

- Review all redetermination details. After reviewing, select “Submit” to finalize the redetermination, select “Edit” to return to the form to make changes, or select “Cancel” to cancel the redetermination and return to the claim detail page.

- If “Submit” was selected, the Request Redetermination – Confirmation page will load and also provide a tracking number. Make a note of the number for your records or, if you wish to have a printed copy of the redetermination, press the Print button. To close the Confirmation pop up box, select the Close button and the claim detail page will reload.
APPEAL STATUS

- Use the Appeal Status search to locate the status of previously submitted Part A or Part B redeterminations, regardless of how they were submitted. Status information is normally available within 15 days of the received date. Click “Appeals Search” from the left-hand navigation bar.

On the Appeal Search page, two tabs will be available. Choose Part A/B Appeal.

- Select the Service Location (NPI), add the patient’s Medicare number, first initial of patient’s first name, and patient’s full last name.

- For Part A claims, enter only a valid date of service range. For Part B claims, enter either a valid claim number (ICN) or date of service, not both. Then click “Search.”

- The Appeals Results page appears and will display the details that were entered as well as any claim results found. The results can be filtered by beginning to type in the Filter box (1) or sorted by clicking the small arrows next to the headings (2). For Part A, the results page includes all status information available. For Part B only, click on the claim number link to view the appeal status (3). Use the show entries (4) drop down to change.
the number of results shown.

- For Part B only, after clicking the claim number for more information, the Part B Appeal Status page is displayed. The details will again be displayed, with any appeal status information listed below that, including correspondence control number (CCN), adjustment claim number if applicable, correspondence type, receipt date, status, decision date, and decision. This is also sortable and filterable.

Please note:
If your correspondence resulted in an Adjustment, please follow the link in the column "Adjustment Claim Number" to view the status/payment of this Adjustment.

Portal Submitted Appeals
- Use the Portal Submitted Appeals search to locate status and responses to Part B appeals that were submitted directly through the WPS GHA portal. To begin, click “Appeal Search” from the left-hand navigation bar.
On the Appeal Search page, two tabs will be available. Choose the “Portal Submitted Appeals” tab.

The Portal Submitted Appeals page includes informational links and a Reconsideration form link above, and two ways to search below. You can search by entering a valid CCN, ICN/DCN, or Tracking number. Alternatively, you can search with details from the appeal. Click “Search” to move to the next step or “Clear Form” to clear all data from form.
After submitting, you will be brought to the Appeal Results (Part B Appeal) page. The details entered will be at the top, along with results, if any, at the bottom. The results will include Tracking Number, Subject, ICN, Status, and Submit Date. The list can be sorted using the arrows next to the headings (1) or filtered by using the filter box (2). Click on the tracking number or subject link (3) to view the Appeal Response Detail pop-up page. Use the show entries (4) drop down to change the number of results shown.
The Appeal Response Detail page is made up of 3 sections:

- The Appeal Response Detail section, which includes details of the claim and appeal, along with the current status of the appeal.

- The More Information Section, which includes all of the details submitted with the redetermination.
Lastly, the Appeal Decision section. This includes the decision, reason, and response, if available. You can print with the “Print” button or close the pop-up with the “Close” button if finished.
Troubleshooting

Clearing Cache and Internet Cookies

As a rule, a WPS GHA Portal user should never save the WPS GHA Portal URL as a favorite. When updates are made to the WPS GHA Portal the saved version is not up to date and can cause issues with logging into the WPS GHA Portal or password errors. Users should always access the WPS GHA Portal via the https://www.wpsgha.com URL or WPS GHA Medicare website.

If a user is having problems accessing the WPS GHA Portal, getting locked out, or having difficulty changing a password, do not use a saved URL and follow the steps below.

- Select the Tools option in the browser’s menu bar.
- Select Internet Options which will pop open another window.
- Select the General tab and look for Browsing history section.
- Select Delete button under Browsing history section.
- Select which times to delete.

We recommend only having the User select temporary files and/or cookies to delete. There may be some users that do not have the rights to do this and would need to contact their Internal IS department for assistance.

WPS GHA Portal Eligibility Discrepancy

The WPS GHA Portal uses the CMS HETS 270/271 eligibility transaction which is different than CWF. When the WPS GHA Portal shows a different Medicare number or Name than CWF, a Medicare card or a Provider Record please follow the below steps to research. WPS GHA cannot make changes to these records, that patient would need to contact the Social Security Administration to make sure all records get updated.

Qualified Medicare Beneficiary (QMB) Helpful Information

When a patient is enrolled in a QMB period you will want to look at the QMB tab, NOT the Summary tab, for the QMB time period. Outside of the QMB enrollment periods, you can look at the Summary, Part A Deductible and Part B Deductible tabs. Be aware that Medicare deductible, copay, and other days will show as effective during non-QMB periods. The QMB tab will provide:

Dual Eligibility Entitlement Enrollment Period

- Part A Entitlement
  - Part A Deductible Amount for the period (zero)
  - Inpatient Spell Days Beginning and Remaining
  - Inpatient Spell Effective and Termination Dates
  - Inpatient Spell Days Co-Payment (zero)
  - Inpatient Spell Days Co-Payment Effective and Termination Dates
  - Part A SNF Days Beginning and Remaining
  - Part A SNF Co-Payment Effective and Termination Dates
  - Part A SNF Days Co-Payment (zero)
Part B Entitlement
- Part B Deductible Amount for the Period (zero)
- Part B Deductible Effective and Termination Dates
- Part B Co-Insurance Amount for Period (zero)
- Part B Co-Insurance Effective and Termination Dates

Recertification Requirements

Annual re-certification is required in the WPS GHA Portal. Beginning 90 days from recertification, upon log in, the user will receive a message on their Dashboard page with the date that Recertification must be completed by. At that time, the User may recertify or choose to wait until later. Failure to complete the re-certification process before the due date will result in the User account being permanently disabled. Disabled accounts cannot be re-activated, and the User will have to register with a new User ID.

- When a User is ready to re-certify they will select “Recertify” located on their WPS GHA Portal Dashboard.
- The User must read and accept or decline the user agreements. If User declines either, the account is permanently disabled. To accept they must click I accept in the Transactional and General boxes and click in the “I have read and agree to abide by these Terms of Use for Transactional Areas. I understand that acceptance provides Medicare with an electronic signature.” Statement. Then click “Next.”
- If the User accepts the user agreement, they must then attest to the Annual Security Awareness Training. If User selects “No” this will disable the account permanently.
- If the User selects “Yes” to the Annual Security Awareness Training they must enter the Provider Credential Information they are currently approved to access: NPI, PTAN, and TIN and then click “Next.”
- The User is then required to enter financial information from a current remit for an NPI they are recertifying for. It can be a combination of a Patient’s Medicare Number and Date of Service or Check/EFT Number or Claim number. Remit must be at least 14 days old but no more than 30 days old. Once entered click “Next.”
- The User is allowed at this point to update profile data such as Name, physical work location, work telephone number and current email address. They must enter their email address in the Confirm email box and select the state of their work location address and then click on “Next.”
- The User is then required to select three new Forgot Password Question and Forgot Password Answers. Then click “Next.”
- Non-Administrators will receive “Recertification Complete” message and select Finish. Administrators must recertify their NPI Administrator Role Responsibilities and then select “Finish.”

Once all steps are completed you will receive a recertification message, click “OK.”

WPS GHA Portal Appeal Statuses

When an appeal is submitted through WPS GHA Portal, the user can track the case status. Below is the listing of the appeal statuses and what the status means.

Redetermination Status
- **Closed** – Your redetermination or reopening was reviewed and has been completed and closed.
- **In Process** – The case has been assigned to be worked
- **Not Accepted** – If any of the documents are not accepted, (this could be 1 document within a zip file containing 10 documents) the entire case would not be accepted, and the user needs to resubmit. This failed virus scanning
- **Pending** – Redetermination or Reopening has been received and is currently pending assignment to a representative.
- **Submitted** – Your redetermination or reopening has been entered in the WPS GHA Portal.

### Frequently Asked Questions (FAQs)

**Q.** Who can register in WPS GHA Portal?

**A.** Providers within the WPS GHA jurisdictions can register for the portal.

Medicare Part B – J5 (IA, KS, MO, NE)
Medicare Part B – J8 (IN, MI)
Medicare Part A – J5 (IA, KS, MO, NE)
Medicare Part A – J8 (IN, NE)
Medicare Part A – J5 National

**Q.** What NPI needs to be used to register for a portal account?

**A.** The WPS GHA Portal is based on the Group NPI and a user must register using the Group NPI, not the individual NPI.

**Q.** How recent does a remit need to be to register or recertify in WPS GHA Portal?

**A.** The remit should have a current date within the last 30 days for recertification and must be for one of the NPI(s)/PTAN(s) that the user has access to. For registration it must be for the NPI/PTAN that you are registering for.

**Q.** Who must register a user in WPS GHA Portal?

**A.** Any provider wishing to register for the WPS GHA Portal may self-register. However, the NPI Administrator may register new users also.

**Q.** How do I locate a current NPI WPS GHA Portal Administrator?

**A.** On the Secure Login page on the portal, under the Registration section, enter the NPI, PTAN and TIN and click Submit. The user will be provided the Name, phone number and email address for the Administrator(s).

**Q.** Does an Administrator create a password for a new user account they created?

**A.** When an Administrator creates a new user account, the user will receive an email with a temporary password. It is the responsibility of the Administrator to give the new user their User Login ID.

**Q.** Is there a limit to the number of Administrators that can be associated to an NPI?

**A.** There is **NO** limit to the number of Administrators that can be associated to an NPI. However, only the very first two can self-register. All additional Administrator access requests must be submitted through Secure Message.
Q. If an account locks because of entering a password incorrectly three times, how do we get it unlocked?
A. User accounts will unlock after three (3) hours. The user should contact their Administrator to reset their password and the account will immediately unlock.

Q. Who can request a Redetermination through WPS GHA Portal?
A. Medicare Part B providers who submit claims for services performed in our J5 jurisdiction (Iowa, Kansas, Missouri, Nebraska), and our J8 jurisdiction (Indiana and Michigan) can submit an appeal through the WPS GHA Portal

Q. What is the WPS GHA Portal remit process?
A. One of the goals WPS GHA has is to reduce the number of providers receiving the standard paper remit and increase the number of providers who receive an ERA. However, many of our SPR providers are not able to migrate to the ERA format and the WPS GHA Portal remit process allows providers to get their remits in an electronic format they can access. Benefits for the provider are:

- The WPS GHA Portal remit process is faster
- Is more secure then the paper RA option
- You have immediate access to your remits without any mail delays.
- It's FREE!

Q. How will I know when a remit is available?
A. Providers can use the "Checks" option on the IVR to identify all of the checks/remits issued within a date range. By selecting "range of dates" when prompted the IVR will provide the total number of checks/remits issued during the date range. This includes both regular and no-pay remits. Another option is to check WPS GHA Portal to see if anything was issued on a specific date by entering that date or date range in the duplicate remit request option (from the left navigation). Additional information on using the "Checks" IVR feature is available in the IVR Operating Guide on our website.

Q. Is there a guide that I can follow to retrieve my remits?
A. The duplicate remit instructions in the WPS GHA Portal User Manual provide guidance on how to retrieve the remits.

Q. I enrolled in WPS GHA Portal Remits, so I get electronic remits, right?
A. Providers enrolled in WPS GHA Portal remits are considered SPR providers. Although you have sent an enrollment form to EDI you are not considered ERA because you do not receive an 835-outbound file.

If you would like to change from WPS GHA Portal to ERA visit our Topic Center on our website under the Claims tab and then The Medicare Remittance Advice link. You may also call and discuss the process with the EDI helpdesk staff.

Q. I signed up for WPS GHA Portal remits but have changed my mind. What do I do?
A. You need to call the EDI help desk. They can assist in changing their status back to the standard paper remit.
Q. Can offsets (WO) be obtained on a duplicate remit?
A. Yes, select the Remit Search link from the left-hand navigation. The user would need to drop the first two digits of the FCN and then enter that number in the ICN/DCN field. WPS GHA Portal will display all remits associated to the ICN.

Q. Can special check remits (ERX, HPSA, etc.) be obtained through WPS GHA Portal.
A. No, these will be mailed to the providers.

Q. If an account becomes deactivated, can the user re-register?
A. Yes, the user or the NPI Administrator will need to create a new account.

Q. What happens if you deactivate an NPI Administrator’s account?
A. If this was the only NPI Administrator, then all users who have access to the NPI, will receive a message on their WPS GHA Portal Dashboard indicating the number of NPIs that are in Blackout. Click on the link “Go to My Service Locations” to see what NPIs are in Blackout. A user would still be able to continue using the NPI for 30 days. If after 30 days, there is still no NPI Administrator, then all users will lose access to that NPI.

Q. What is the Annual Security Awareness Training that needs to be attested to during re-certification?
A. The WPS GHA Portal requires all users to attest that they have or will be completing their company’s annual security awareness training. The user’s organization determines the appropriate content of the training. The content includes a basic understanding of the need for information security and the need for operations security.

Q. My account shows inactive, can it be reactivated?
A. Yes, an account can be reactivated by the NPI Administrator.

Q. My account shows I have a duplicate/replicated account, who can fix this?
A. You need to contact the Customer Service Department to have this fixed.

Q. I am leaving my job and need to disable my account, how do I do this?
A. You can go to “My Profile” page in the portal and click the disable button or contact the Customer Service department.

Administrative Access FAQs

Q. How does a new or current user obtain Administrator access to an NPI?
A. Depending on the situation, the following are the most common issues and resolutions.

Only one (1) NPI WPS GHA Portal Admin:

- If the user **Does Not** have an account and there is only 1 Admin, you will need to register for an account and accept the Administrator Role and Responsibilities and you will obtain immediate Admin access.
- If the user has an account with access to the NPI, remove the NPI from My Service Locations (NPIs). Then request access to the NPI by entering the NPI, PTAN, TIN by clicking on the + Request Access button at the top of the My Service Locations page, Accept the Role of Administrator, and enter current financial information. The user will obtain immediate Administrator access.
If the user has an account but does not have access to the NPI, you need to request access to the NPI by entering the NPI, PTAN, TIN by clicking on the + Request Access button at the top of the My Service Locations page, Accept the Role of Administrator, and enter current financial information. The user will obtain immediate Administrator access.

Two (2) or more NPI WPS GHA Portal Administrators and the user Does Not have an account:

- If the user Does Not have an account and the Administrator is still valid, the user needs to work with their Administrator(s) to have an account created or self-register. Once the account has been created, the Administrator would request Administrator access for that user by submitting a secure message via the Message Center in the left-hand navigation. This could take up to 45 days to obtain the access. Account access is immediate.
- If the user Does Not have an account and the Administrator(s) are no longer valid, the user will need to contact the Call Center for assistance.

Two (2) or more Administrators and the caller has an account:

- If the user has an account with access to the NPI in question, and if the Administrator(s) are valid, the caller should work with their Administrator(s) to have a request submitted for the Administrator access. Inform the caller that this can take up to 45 days to obtain Admin access.
- If the user has an account but does not have access to the NPI in question, and if the NPI WPS GHA Portal Administrator(s) are valid, the caller should work with their Administrator(s) to obtain access to the NPI in question and then have the Administrator submit a request for the Administrator access through secure message. Inform the caller that this can take up to 45 days to obtain the access. Access to the NPI is immediate.
- If the user has an account with access to the NPI in question, but the NPI WPS GHA Portal Administrators are not valid, contact Customer Service for assistance.
- If the user has an account but does not have access to the NPI in question, and if the NPI WPS GHA Portal Administrators are not valid, contact Customer Service for assistance.

Username FAQs

Q. Is a User Login ID case sensitive?
A. No it is not, only passwords are case sensitive.

Password FAQs

Q. Can Customer Service help if the user cannot remember their password?
A. Yes, however, the user would need to provide information to validate they are the user and then Customer Service can generate a temporary password email to the user.
Q. Can an Administrator call Customer Service to have one of their user’s password reset?
A. Yes, but first the Administrator would need to provide information to verify they are the Administrator and then verify that the person is linked under that Administrator. However, the Administrator can also reset the user’s password.

Q. I received the following error message when trying to change my password on the Password expired page "The client supplied invalid authentication information" what does this mean?
A. The user entered the old password incorrectly in the “Current password” field.
****Note: **** If there are ***** in the field, delete these and enter the temporary password from the password reset email.

Q. I received the following error message when trying to change my password on the Password expired page "New password verification failed. Make sure the new password fields contain the same data" what does this mean?
A. The new password and confirm new password fields do not match. Different passwords were typed in each field.

Q. I received the following error message when trying to change my password on the Password expired page "Password rejected due to policy violation" what does this mean?
A. The new password does not meet all the password requirements. Most common errors when creating a new password is entering dictionary words and/or not using one of the four listed special characters listed on the screen (# $ % &).

Q. When a password is reset, how long is the temporary password valid?
A. The temporary password is valid for 21 days. If you do not utilize the temporary password within 21 days, the account is disabled and a new one will need to be created.

Claim Entry FAQs

Q. How can a claim be submitted via WPS GHA Portal?
A. See “Register for Online Claim Entry” in this manual.

Non-Assigned Providers FAQs

Q. Can a non-assigned provider register for WPS GHA Portal?
A. Yes, a non-assigned provider may register to use WPS GHA Portal.

Q. What Claims Status information is available for a Non-Assigned provider to see?
A. WPS GHA Portal will display the following claim information on non-assigned claims:
   - If the claim was received
   - Beginning and end dates of service
   - Claim status (In Process, Approved, Denied, Rejected)
   - Processed/finalized date

Appeals FAQs

Q. Who can view an Appeal in WPS GHA Portal?
A. Any standard user or Administrator under the NPI the appeal was submitted under may view the appeal in WPS GHA Portal.
# Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>12/29/2016</td>
<td>Adding new manual with Revision History page.</td>
</tr>
<tr>
<td>2.0</td>
<td>3/24/2017</td>
<td>Added text to password 21-day rule. Added text for Administrator disabling accounts. Change screens with Appeal Status tab order. Remove G0389 and replace with 76706 in Preventive Services for eligibility. Added Multi-Factor Authentication section.</td>
</tr>
<tr>
<td>3.0</td>
<td>05/24/2017</td>
<td>Updated “Request Submitter ID” section to be “Register for Online Claim Entry” There is a new process for user to enroll in online claim entry using the portal. Updated screen shots and text to explain the new process</td>
</tr>
<tr>
<td>4.0</td>
<td>07/18/2017</td>
<td>Added information to the MFA section concerning the roll-out and updates that were not made on 05/24/2017.</td>
</tr>
<tr>
<td>5.0</td>
<td>09/05/2017</td>
<td>Added new screens for new claim inquiry features. Updated MFA showing code is now valid for 4 hours and also on how to change default to Google Authenticator. Added new screens for new Provider Self Service Denial tool.</td>
</tr>
<tr>
<td>6.0</td>
<td>10/02/2017</td>
<td>Corrected some MFA screens.</td>
</tr>
<tr>
<td>7.0</td>
<td>01/26/2018</td>
<td>Replaced the entire MFA section. Code is now valid for 8 hours and screens changed.</td>
</tr>
<tr>
<td>8.0</td>
<td>03/09/2018</td>
<td>Updated Administrator Roles, QMB information, added FAQs. New screens showing the new Appeals Tabs.</td>
</tr>
<tr>
<td>9.0</td>
<td>04/01/2018</td>
<td>Added MBI information.</td>
</tr>
<tr>
<td>Version</td>
<td>Date</td>
<td>Description of Changes</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10.0</td>
<td>04/23/2018</td>
<td>Changed the Name of the MBI section.</td>
</tr>
<tr>
<td>11.0</td>
<td>06/15/2018</td>
<td>Added Easier Remittance Advice lookup, Who is My Admin feature, new NPI Admin Lookup on login page, added MDPP information.</td>
</tr>
<tr>
<td>12.0</td>
<td>08/31/2018</td>
<td>Re-wrote Message Center adding in Audit.</td>
</tr>
<tr>
<td>13.0</td>
<td>11/02/2018</td>
<td>Modified the Clerical Error Reopening (CER) section. Renamed to match Link in Footer of Portal.</td>
</tr>
<tr>
<td>14.0</td>
<td>11/15/2018</td>
<td>Added section to remove access for Standard and Eligibility Users.</td>
</tr>
<tr>
<td>15.0</td>
<td>11/20/2018</td>
<td>Removed numbered lists and replaced with bulleted lists for easier formatting.</td>
</tr>
<tr>
<td>16.0</td>
<td>03/30/2019</td>
<td>Added Account Reactivation section and updated eligibility section with HETS Q100 changes.</td>
</tr>
<tr>
<td>17.0</td>
<td>04/22/2019</td>
<td>Updated Financial data timeframe from 90 to 30. Added a note to the account reactivation section.</td>
</tr>
</tbody>
</table>

**WPS GHA Medicare eNews Messages**

Stay up to date on Medicare issues by signing up for our free WPS GHA Medicare eNews. By subscribing, you can enjoy a free, easy, and secure way to stay current on the latest Medicare information, with the option to unsubscribe at any time. To receive our eNews Messages, go to [https://corp-ws.wpsic.com/apps/commercial/unauth/medicareListservUserWelcomeLoadAction.do](https://corp-ws.wpsic.com/apps/commercial/unauth/medicareListservUserWelcomeLoadAction.do) to subscribe. Then simply check your email regularly to receive the latest Medicare information.