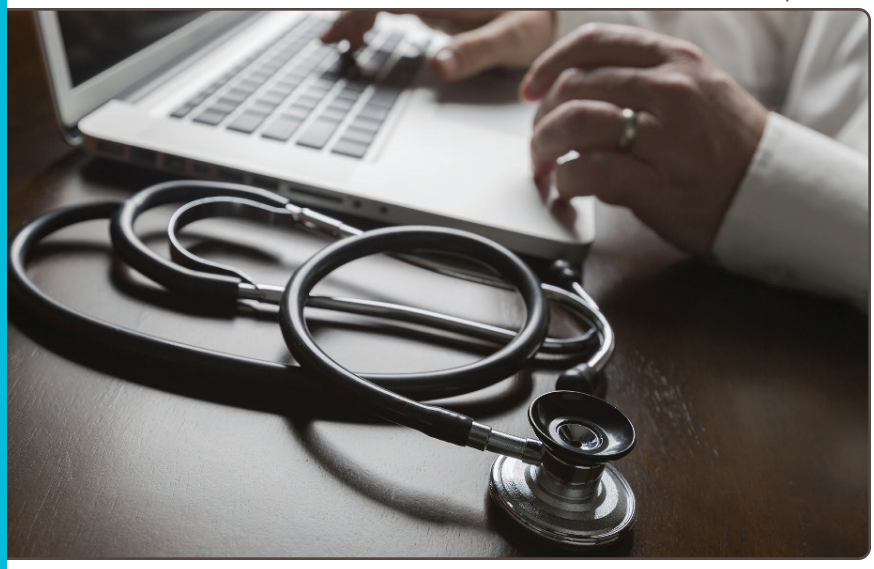
myCGS
DME MAC
JURISDICTIONS B & C

REGISTRATION & ACCOUNT MANAGEMENT GUIDE



DME MAC JURISDICTION B & JURISDICTION C

Contents

Overview

Welcome to the myCGS Registration and Account Management Guide. This guide provides an overview of the registration and account management process that DME MAC Jurisdiction B and C suppliers must follow in order to use myCGS.

In order for your company to use myCGS, you will first need a Designated Approver (DA)—an individual designated as being responsible for approving and managing your organization's employees within myCGS—to successfully complete registration. The DA can be any member of your organization, but is typically an individual who manages other employees that need to use myCGS. The first person to register in myCGS for any supplier must be the DA. No other users for your company can use myCGS until the DA has been registered and approved. There is no limit to the number of DAs that may register for your organization.

Once a DA (or multiple DAs) completes myCGS registration, they will have full access to myCGS and have the ability to approve and manage other myCGS users. Other users from your organization, known as End Users, may then register for myCGS and are approved by their DA. Once approved, End Users will have full access to myCGS.

NOTE: myCGS also offers the ability to register as a third-party biller via the Clearing House/Billing Agent (CHBA) role. Refer to the CHBA sections in this guide for instructions on registering as a CHBA.

Registration for myCGS is completed based on your organization's Tax ID (TIN). Once you have successfully registered under your Tax ID, all of your associated NPI/PTAN combinations will automatically be tied to your account and available for use in myCGS. If your organization has more than one Tax ID, you will need to add your additional Tax IDs by following the instructions in the ***Adding Additional Tax IDs*** section found below.

This guide provides details of each part of the registration and user management process. It is divided into three main sections:

- Section 1 details user registration.
- Section 2 includes instructions for Designated Approvers on how to manage users in myCGS.
- Section 3 includes information about maintaining your myCGS account.

CGS
A CELERIAN GROUP COMPANY

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Originated July 1, 2016 | Revised April 25, 2022

For instructions on using myCGS to obtain beneficiary eligibility, claim status, and all the other features that myCGS offers, refer to the *myCGS User Manual* (https://www.cgsmedicare.com/jc/mycgs/pdf/mycgs_UserManual.pdf).

SECTION 1: Registration

Roles & Definitions

What is a Designated Approver? What is an End User? What is a CHBA?

A **Designated Approver (DA)** is an individual designated by their organization as being responsible for approving and managing your organization's employees within myCGS. A DA must be the first person to register for your organization for myCGS. Once successfully registered, the DA is responsible for approving and maintaining other users from their company in myCGS. DAs also have access to all of the features in myCGS that End Users use (beneficiary eligibility, claim status, etc.).

An **End User** is a regular (non-approver) user of myCGS. End Users are able to use all of the main functionality within myCGS, including beneficiary eligibility, claim status, claim preparation information, and more, but do not have the approver ability of a DA. End Users are approved and maintained by their DA. Once an End User has submitted a registration request in myCGS, a DA must approve the individual for use of the company's Tax ID (and all associated NPIs/PTANs) in myCGS.

A **Clearing House/Billing Agent (CHBA)** is a third party biller who provides authorized services to a DMEPOS supplier. CHBAs are able to use the main functionality within myCGS on behalf of the suppliers they represent. CHBAs are approved for myCGS based on a supplier's Trading Partner Agreement with CEDI, which provides both a Trading Partner ID used in registration, as well as defined access within the portal. For this reason, the DMEPOS supplier must authorized the CHBA by submitting a CEDI Supplier Authorization Form to CEDI **BEFORE a CHBA is able to register for myCGS**. For instructions on submitting the form, refer to the CEDI website (https://www.ngscedi.com/).

For instructions on registering for myCGS as a DA, End User, or CHBA, refer to the sections below.

How to Register as a Designated Approver

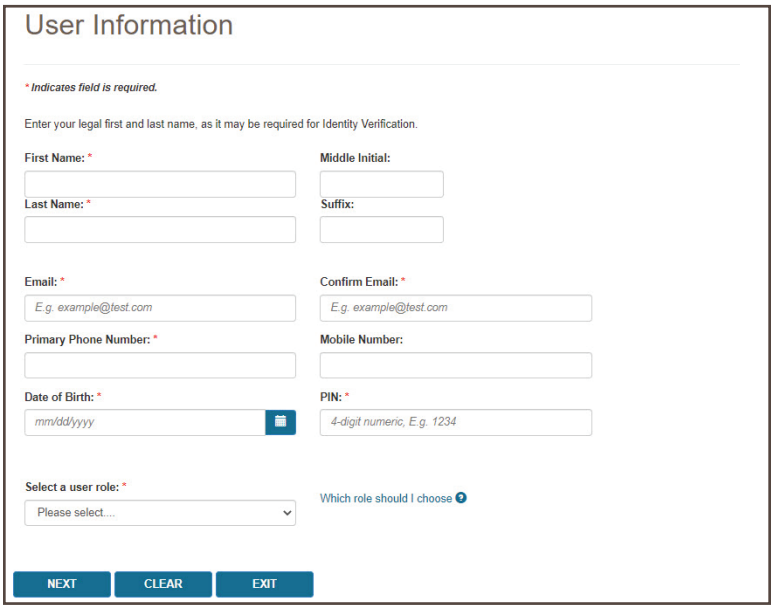
Before you begin registration as a Designated Approver (DA), you will need to have the following information available:

- Your company's Tax ID, along with a PTAN and NPI combination that is tied to the Tax ID.
- The check number and dollar amount of a recent check that has been sent to your company by CGS DME MAC Jurisdiction B or C (either jurisdiction is fine, as long as it's B or C). The check must match your NPI/PTAN, and must be one of the last 50 checks your company has received from CGS within the past 12 months. Note that if you are a new supplier and have not yet billed claims to CGS, you will need to bill at least one claim to Jurisdiction B or C before you can register for myCGS. CMS requires web portal access be limited to suppliers who actively bill DMEPOS claims.

Once you have this information gathered, follow the steps below to register for myCGS as a Designated Approver.

1. Go to myCGS at https://mycgsportal.com.
2. Press the **Register for myCGS** button.
3. The User Information page will display. Enter all appropriate information, including your name, email, phone, date of birth, and a 4-digit Personal Identification Number (PIN) of your choosing.

IMPORTANT: Be sure that you choose a PIN that you will remember—you will need your PIN if you ever forget your myCGS User ID.



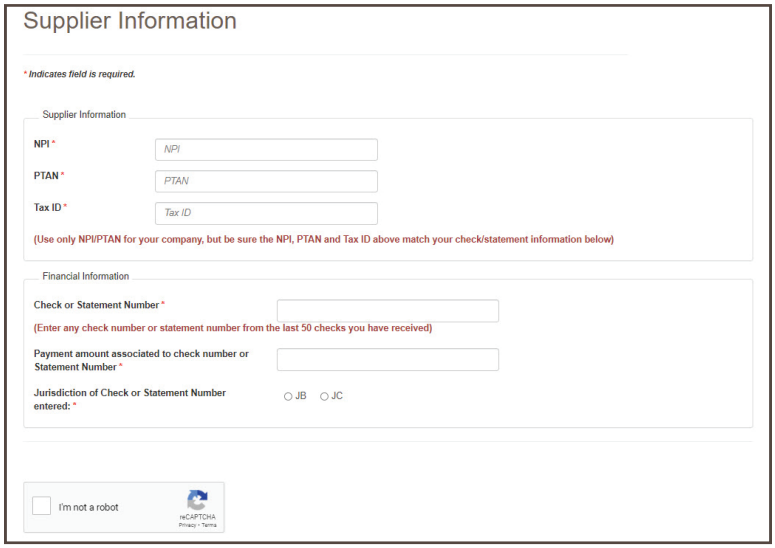
4. In the “Select a user role” field, choose **Designated Approver** from the drop-down menu. After entering your information and choosing your role, press the ***NEXT*** button.

5. The Supplier Information page will display. Enter your NPI, PTAN, and Tax ID. If you have multiple NPIs/PTANs, simply choose any one of them to enter—all of the NPIs/PTANs associated under your Tax ID will automatically be added to your account upon successful registration. Note that if you have more than one Tax ID, you will need to add the additional Tax IDs after you register (refer to the Adding Additional Tax IDs section below).

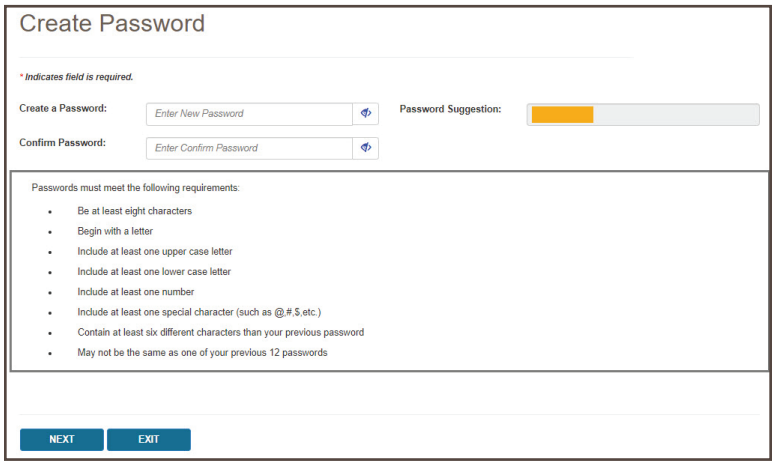
   In the “Check or Statement Number” and “Payment amount associated to check number or statement number” fields, enter the check/EFT number or statement number and dollar amount of one the 50 most recent checks issued to you by CGS DME MAC Jurisdiction B or C. Also select the Jurisdiction (JB or JC) of the check. The check must match the NPI/PTAN you’ve entered on the page.

   Complete the reCAPTCHA field, and then press ***NEXT***.

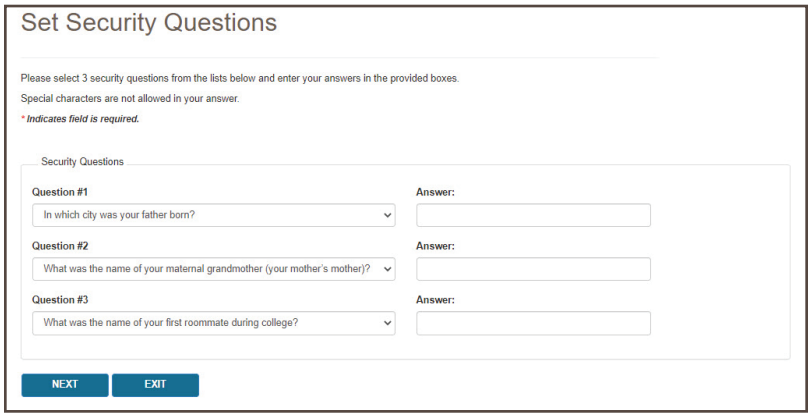
   NOTE: Once you’ve completed the reCAPTCHA field, you must press the NEXT button within one minute or else the verification will expire. If the reCAPTCHA verification does expire, simply complete the field again and then press NEXT.



6. You will then be taken to the Create Password screen. Select a password using either the optional Password Suggestion shown on the screen or a password of your own creation. Once you have confirmed the password, press ***NEXT***.



7. Next you will be asked to set up your security challenge questions and answers. Choose questions from each of the three drop down menus, and answer them accurately. Be sure to choose questions and answers that are personal to you and that you will remember. You will need to be able to answer the challenge questions should you forget your password and need to have it reset.

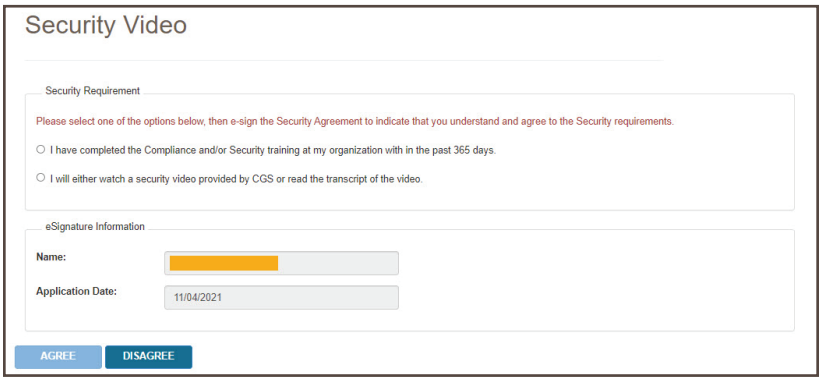


NOTE: The security question answers are case-sensitive. Be sure to remember if you use capital vs. lower case letters in your answers.

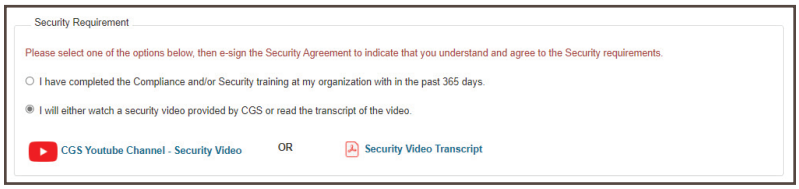
Once you have selected your questions and entered your answers, press the button.

8. After setting your security questions, you will be taken to the Terms of Use & eSignature Information screen. Your name and today's date will automatically populate in the eSignature Information section at the bottom of the page. Read the terms of use carefully. If you agree to the terms of use, press the AGREE button. Note that if you disagree, your registration request will be cancelled. You must agree to the terms of use in order to use myCGS.

9. You will then be taken to the Security Video screen. CGS requires that all myCGS users complete annual compliance/security training in order to ensure that our users are familiar with best practices related to protecting both beneficiary and supplier information, as well as your own personal information. If your company provides annual compliance/security training which you have taken within the past 365 days, then choose the first option on the screen and press the AGREE button.



If you have not received any compliance/security training within the past 365 days, then select the second option. This will present you with the option of either watching a security video provided by CGS or reading the transcript of the video. Note that the security video is approximately 12 minutes in length.



After you have either watched the video or read the video transcript, press the AGREE button to continue.

Note that if you disagree, your registration request will be cancelled. You must agree to complete annual compliance/security training in order to use myCGS.

10. After pressing AGREE on the Security Video screen, you will receive a Submission Successful message, including your new myCGS User ID. You will also receive a confirmation email containing your User ID. Be sure to take note of your User ID, as you will need it every time you log in to myCGS.

11. Although your registration has now been submitted, you still need to complete your myCGS account by setting up your Multi-Factor Authentication (MFA) preferences. To do so, go to myCGS at https://mycgsportal.com, and press the ***Log In to DME myCGS*** button. Then enter your myCGS User ID and password, and press ***SUBMIT***.

12. You will be prompted to set your MFA preferences. You have the option of receiving MFA codes via text, email, or Google Authenticator. We recommend that you set up at least two forms of MFA so that you always have a backup.

    If you choose to use Text as one of your MFA options, you must enter your 10-digit cell phone number, and choose your cell phone service provider (AT&T, Sprint, T-Mobile, or Verizon).

    NOTE: If you use a cell phone carrier other than one of the four service providers listed, choose the service provider network which is used by your carrier to provide service. If you are unsure of the network, please contact your carrier. If you choose the wrong service provider, you will not receive MFA text messages.

    If you choose to use Google Authenticator, you will need to either download the Google Authenticator app on your smart device (phone, tablet, etc.) or add the Google Authenticator extension to your web browser (Chrome, Firefox, or Edge). There are also third-party applications that can give you access to Google Authenticator (CGS does not provide advice on use of third-party applications). Check with your company's IT administrators to see if Google Authenticator can be made available to you and your staff.

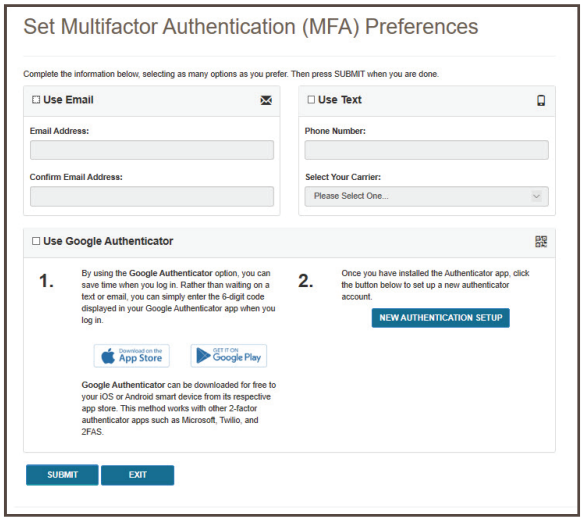
    To use Google Authenticator, first download the appropriate app on your smart device, or download the web browser extension:

    - Apple App Store (https://apps.apple.com/us/app/google-authenticator/id388497605)
    - Google Play (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_US&gl=US)

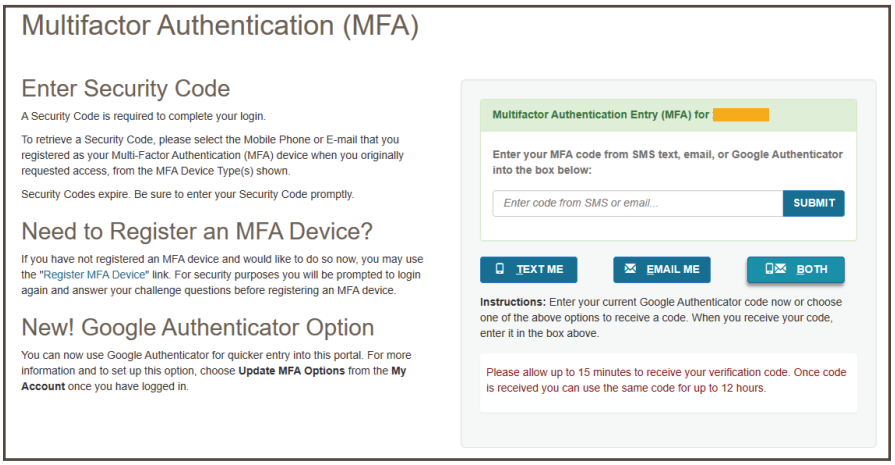
- Google Authenticator Browser Extension (https://authenticator.cc/)

Then select the checkmark next to “Use Google Authenticator,” or press “New Authentication Setup.” A QR code will display on screen. Follow the instructions in your Google Authenticator app or web extension to scan the QR code, or manually enter the code.

After entering your MFA information, press the ***SUBMIT*** button. If you chose Google Authenticator as one of your MFA choices, you will be immediately asked to enter your Google Authenticator code.



13. After setting up your MFA, you will immediately need to log in again and use an MFA security code to continue. On the MFA page, press the ***Text Me***, ***Email Me***, or ***Both*** button, depending on how you wish to receive your MFA security code, or if you are using Google Authenticator, simply enter your current Google Authenticator code. Note that you can use your keyboard (T for text, E for email, or B for both) to select and generate your MFA code. Once you receive the code, enter it in the MFA Code Entry field, and press ***SUBMIT*** (or press Enter on your keyboard).



Congratulations, you have now successfully completed myCGS registration! You are now ready to use myCGS and approve (or reject) End Users for your company. For instructions on using myCGS to find beneficiary eligibility, claim status, and all the other great features myCGS offers, refer to the *myCGS User Manual*.

After you (or another Designated Approver from your company) have successfully completed myCGS registration, End Users from your company may also register for myCGS. When an End User has submitted a registration request under your Tax ID, you will receive an email informing you that you have pending approvals. For instructions on approving and managing End Users from your company, refer to ***SECTION 2: USER MANAGEMENT*** of this guide.

How to Register as an End User

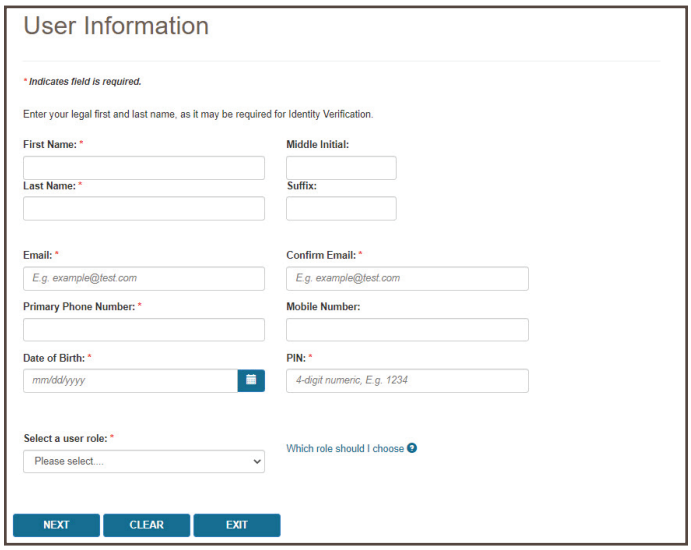
Before you begin registration as an End User you will need to have the following information available:

- Your company's Tax ID.
- A PTAN and NPI combination that is tied to the Tax ID.
- Confirmation that at least one Designated Approver from your company has already registered successfully for myCGS. End Users cannot register in myCGS without a Designated Approver under the same Tax ID.

Once you have this information gathered, follow the steps below to register for myCGS as an End User.

1. Go to myCGS at https://mycgsportal.com.
2. Press the **Register for myCGS** button.
3. The User Information page will display. Enter all appropriate information, including your name, email, phone, date of birth, and a 4-digit Personal Identification Number (PIN) of your choosing.

   IMPORTANT: Be sure that you choose a PIN that you will remember—you will need your PIN if you ever forget your myCGS User ID.

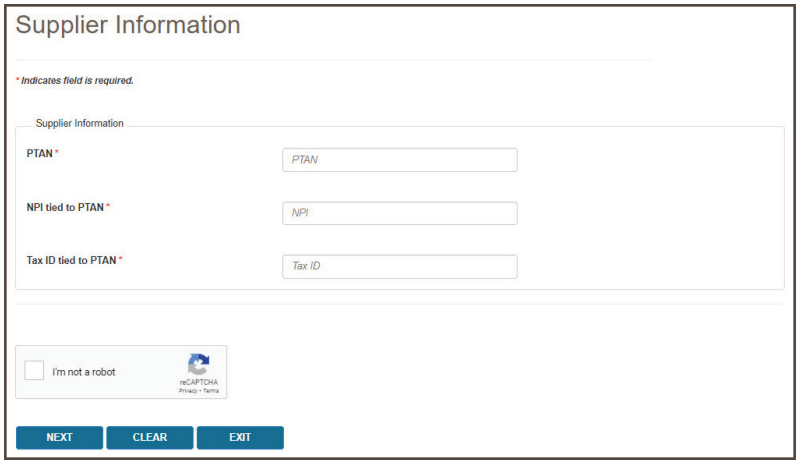


4. In the "Select a user role" field, choose **End User** from the drop-down menu. After entering your information and choosing your role, press the ***NEXT*** button.
5. The Supplier Information page will display. Enter your PTAN, NPI, and Tax ID. If you have multiple PTANs/NPIs, simply choose any one of them to enter—all of the PTANs/NPIs associated under your Tax ID will automatically be added to your account upon successful registration.

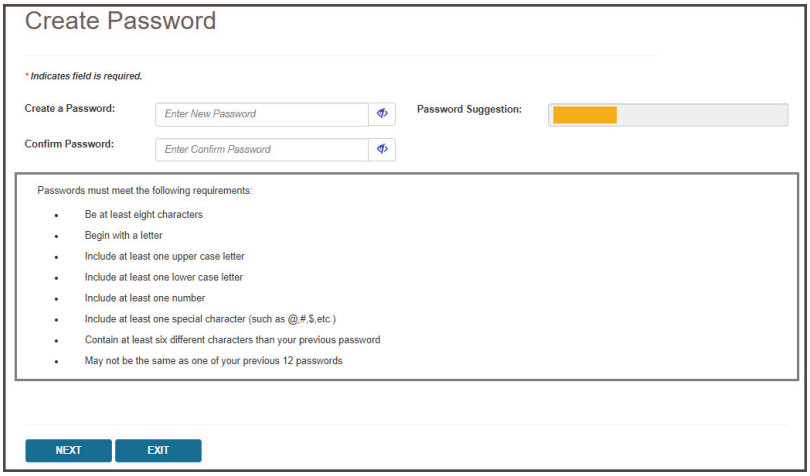
   NOTE: If a Designated Approver has not already successfully registered for myCGS with your company's Tax ID, then your submission will not be accepted (you will receive an error message). You must wait until a Designated Approver has successfully completed registration before you can register.

   Complete the reCAPTCHA field, and then press NEXT.

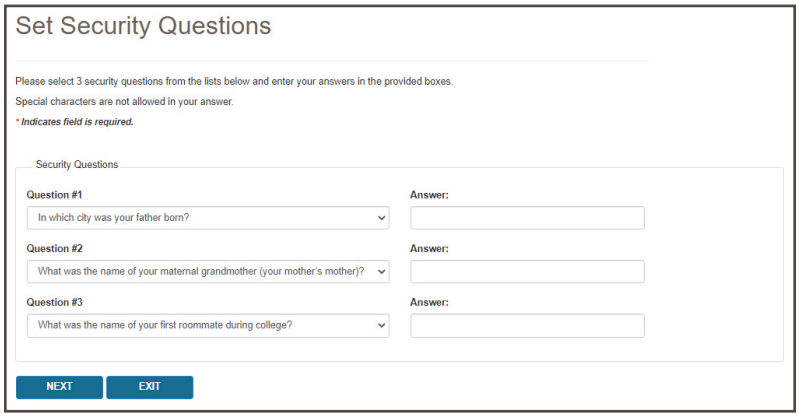
   NOTE: Once you've completed the reCAPTCHA field, you must press the NEXT button within one minute or else the verification will expire. If the reCAPTCHA verification does expire, simply complete the field again and then press NEXT.



6. You will then be taken to the Create Password screen. Select a password using either the optional Password Suggestion shown on the screen or a password of your own creation. Once you have confirmed the password, press ***NEXT***.



7. Next you will be asked to set up your security challenge questions and answers. Choose questions from each of the three drop-down menus, and answer them accurately. Be sure to choose questions and answers that are personal to you and that you will remember. You will need to be able to answer the challenge questions should you forget your password and need to have it reset.

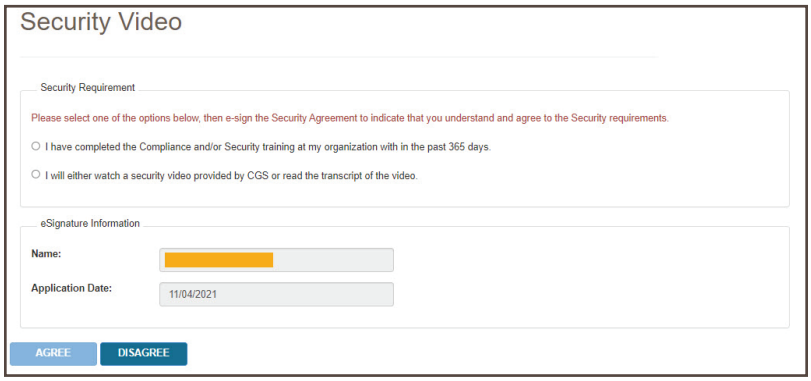


NOTE: The security question answers are case-sensitive. Be sure to remember if you use capital vs. lower case letters in your answers.

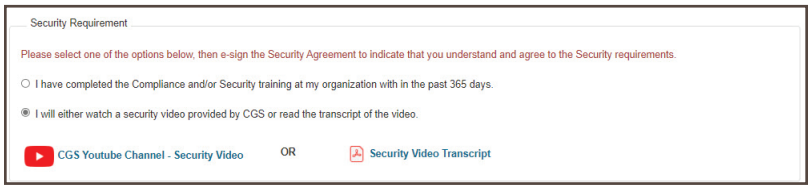
Once you have selected your questions and entered your answers, press the button.

8. After setting your security questions, you will be taken to the Terms of Use & eSignature Information screen. Your name and today's date will automatically populate in the eSignature Information section at the bottom of the page. Read the terms of use carefully. If you agree to the terms of use, press the AGREE button. Note that if you disagree, your registration request will be cancelled. You must agree to the terms of use in order to use myCGS.

9. You will then be taken to the Security Video screen. CGS requires that all myCGS users complete annual compliance/security training in order to ensure that our users are familiar with best practices related to protecting both beneficiary and supplier information, as well as your own personal information. If your company provides annual compliance/security training which you have taken within the past 365 days, then choose the first option on the screen and press the AGREE button.



If you have not received any compliance/security training within the past 365 days, then select the second option. This will present you with the option of either watching a security video provided by CGS or reading the transcript of the video. Note that the security video is approximately 12 minutes in length.



After you have either watched the video or read the video transcript, press the AGREE button to continue.

Note that if you disagree, your registration request will be cancelled. You must agree to complete annual compliance/security training in order to use myCGS.

After pressing AGREE on the Security Video screen, you will receive a message stating that your submission was successful. Your Designated Approver will then need to review your request and approve (or deny) it.

NOTE: Your Designator Approver must approve (or deny) your request within five days. If your Designator Approver does not take action within five days, you will receive an email stating that your request has been removed. If this occurs, you will need to re-register.

When your request has been approved by your Designated Approver, you will receive an approval email with your myCGS User ID. Once you have received your approval email, you must set up your Multi-Factor Authentication (MFA) preferences to complete your myCGS account. To do so, follow these steps:

1. Go to myCGS at https://mycgsportal.com, and press the ***Log In to DME myCGS*** button.

2. Enter your myCGS User ID and password, then press ***SUBMIT***.

3. You will be prompted to set your Multi-Factor Authentication (MFA) preferences. You have the option of receiving MFA codes via text, email, or Google Authenticator. We recommend that you set up at least two forms of MFA so that you always have a backup.

   If you choose to use Text as one of your MFA options, you must enter your 10-digit cell phone number, and choose your cell phone service provider (AT&T, Sprint, T-Mobile, or Verizon).

NOTE: If you use a cell phone carrier other than one of the four service providers listed, choose the service provider network which is used by your carrier to provide service. If you are unsure of the network, please contact your carrier. If you choose the wrong service provider, you will not receive MFA text messages.

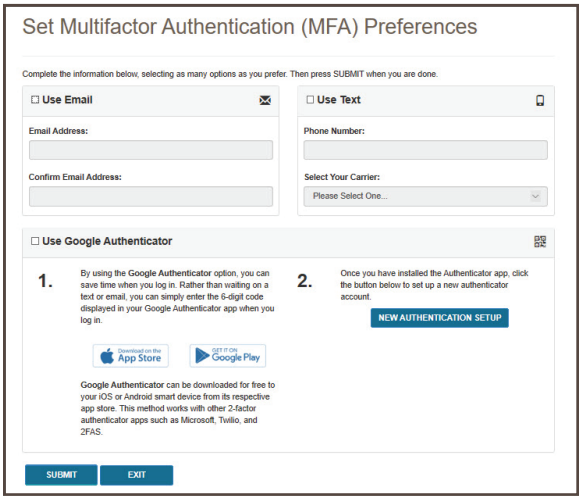
If you choose to use Google Authenticator, you will need to either download the Google Authenticator app on your smart device (phone, tablet, etc.) or add the Google Authenticator extension to your web browser (Chrome, Firefox, or Edge). There are also third-party applications that can give you access to Google Authenticator (CGS does not provide advice on use of third-party applications). Check with your company's IT administrators to see if Google Authenticator can be made available to you and your staff.

To use Google Authenticator, first download the appropriate app on your smart device, or download the web browser extension:

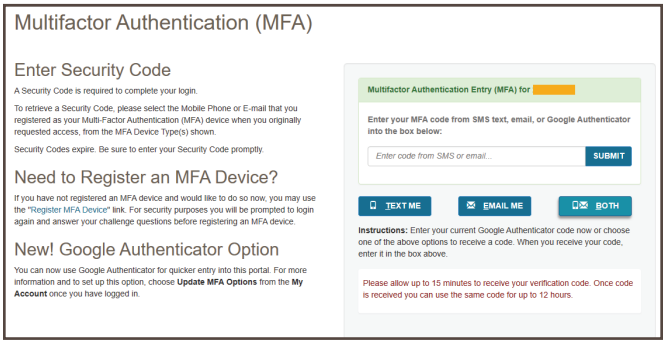
- Apple App Store (https://apps.apple.com/us/app/google-authenticator/id388497605)
- Google Play (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_US&gl=US)
- Google Authenticator Browser Extension (https://authenticator.cc/)

Then select the checkmark next to "Use Google Authenticator," or press "New Authentication Setup." A QR code will display on screen. Follow the instructions in your Google Authenticator app or web extension to scan the QR code, or manually enter the code.

After entering your MFA information, press the ***SUBMIT*** button. If you chose Google Authenticator as one of your MFA choices, you will be immediately asked to enter your Google Authenticator code.



4. After setting up your MFA, you will immediately need to log in again and use an MFA security code to continue. On the MFA page, press the ***Text Me***, ***Email Me***, or ***Both*** button, depending on how you wish to receive your MFA security code, or if you are using Google Authenticator, simply enter your current Google Authenticator code. Note that you can use your keyboard (T for text, E for email, or B for both) to select and generate your MFA code. Once you receive the code, enter it in the MFA Code Entry field, and press ***SUBMIT*** (or press Enter on your keyboard).



Congratulations, you have now successfully completed myCGS registration! You are now ready to use myCGS. For instructions on using myCGS to find beneficiary eligibility, claim status, and all the other great features myCGS offers, refer to the *myCGS User Manual* (https://www.cgsmedicare.com/jc/mycgs/pdf/mycgs_UserManual.pdf).

How to Register as a Clearing House/Billing Agent (CHBA)

Before you can register as Clearing House/Billing Agent (CHBA), the supplier(s) your company represents must authorize your company's usage of DME MAC Web portals on their behalf by completing a CEDI Supplier Authorization Form. The authorization is based on the supplier's Trading Partner Agreement. As a result of that process, your company will receive a Trading Partner ID, which you will need in order to complete myCGS registration. For information about the authorization form, visit the CEDI website (http://www.ngscedi.com/).

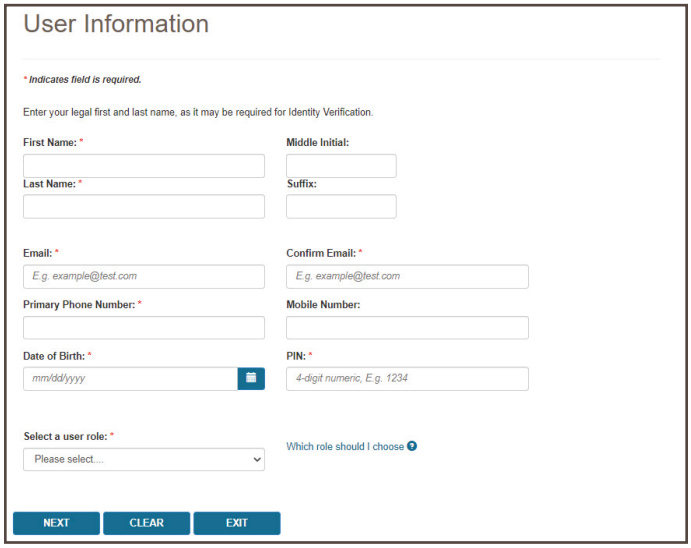
Once your company has been authorized by a DMEPOS supplier to use their Trading Partner ID, follow the steps below to register for myCGS as a CHBA. Before you begin registration as a CHBA user you will need to have the following information available:

- Confirmation that your company has been authorized by a DMEPOS supplier to use their Trading Partner ID.
- The Trading Partner ID(s) your company has been authorized to use.

Once you have this information gathered, follow the steps below to register for myCGS as a CHBA.

1. Go to myCGS at https://mycgsportal.com.
2. Press the **Register for myCGS** button.
3. The User Information page will display. Enter all appropriate information, including your name, email, phone, date of birth, and a 4-digit Personal Identification Number (PIN) of your choosing.

   IMPORTANT: Be sure that you choose a PIN that you will remember—you will need your PIN if you ever forget your myCGS User ID.



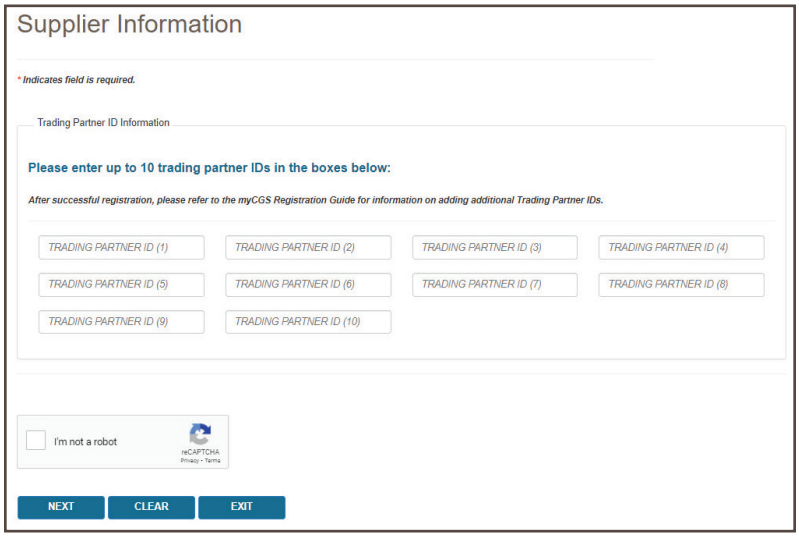
4. In the "Select a user role" field, choose **Clearing House/Billing Agency** from the drop-down menu. After entering your information and choosing your role, press the ***NEXT*** button.
5. The Supplier Information page will display. Enter the appropriate Trading Partner IDs that your company has been authorized to use (up to 10). When you enter Trading Partner IDs, myCGS will immediately validate whether or not they are valid and approved for use by a CHBA. You must enter at least one valid Trading Partner ID in order to complete myCGS registration.

   Note that jurisdictional and functional permissions for each Trading Partner ID are granted by the DMEPOS supplier in their CEDI authorization agreement. If the supplier did not grant CHBAs to have access to a specific jurisdiction (B or C) or function (eligibility, claims, finance, etc.), then you will not be able to access those jurisdictions/functions in myCGS for the associated NPI/PTAN.

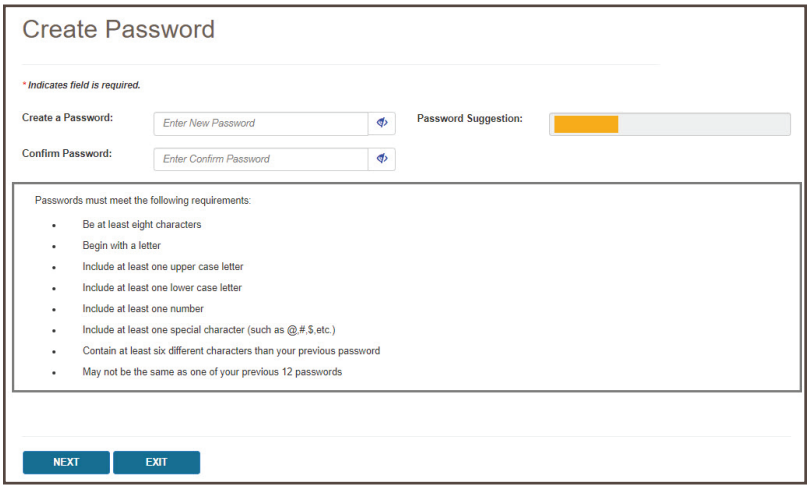
NOTE: If your company represents more than 10 Trading Partner IDs, you can add the rest of the IDs after completing your initial myCGS registration. Refer to the Update Trading Partner IDs section below for instructions.

After entering your Trading Partner ID(s), complete the reCAPTCHA field, and then press ***NEXT***.

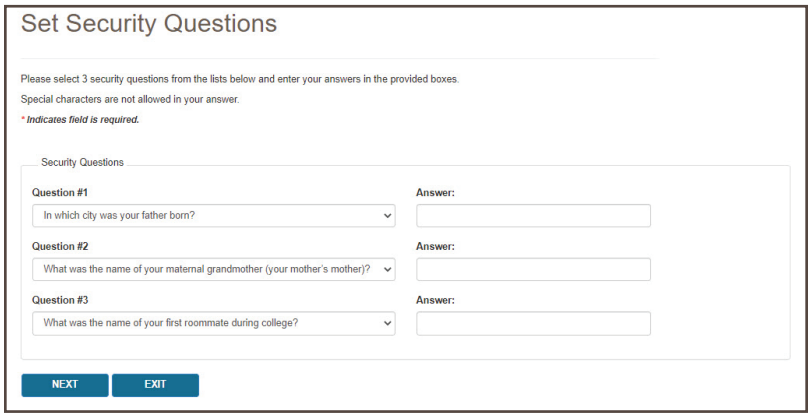
NOTE: Once you've completed the reCAPTCHA field, you must press the ***NEXT*** button within one minute or else the verification will expire. If the reCAPTCHA verification does expire, simply complete the field again and then press ***NEXT***.



6. You will then be taken to the Create Password screen. Select a password using either the optional Password Suggestion shown on the screen or a password of your own creation. Once you have confirmed the password, press ***NEXT***.



7. Next you will be asked to set up your security challenge questions and answers. Choose questions from each of the three drop down menus, and answer them accurately. Be sure to choose questions and answers that are personal to you and that you will remember. You will need to be able to answer the challenge questions should you forget your password and need to have it reset.



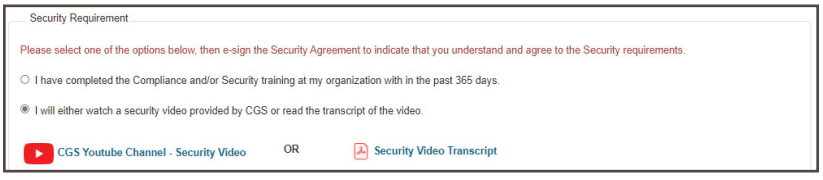
NOTE: The security question answers are case-sensitive. Be sure to remember if you use capital vs. lower case letters in your answers.

Once you have selected your questions and entered your answers, press the button.

8. After setting your security questions, you will be taken to the Terms of Use & eSignature Information screen. Your name and today's date will automatically populate in the eSignature Information section at the bottom of the page. Read the terms of use carefully. If you agree to the terms of use, press the AGREE button. Note that if you disagree, your registration request will be cancelled. You must agree to the terms of use in order to use myCGS.

9. You will then be taken to the Security Video screen. CGS requires that all myCGS users complete annual compliance/security training in order to ensure that our users are familiar with best practices related to protecting both beneficiary and supplier information, as well as your own personal information. If your company provides annual compliance/security training which you have taken within the past 365 days, then choose the first option on the screen and press the AGREE button.

If you have not received any compliance/security training within the past 365 days, then select the second option. This will present you with the option of either watching a security video provided by CGS or reading the transcript of the video. Note that the security video is approximately 12 minutes in length.



After you have either watched the video or read the video transcript, press the AGREE button to continue.

Note that if you disagree, your registration request will be cancelled. You must agree to complete annual compliance/security training in order to use myCGS.

10. After pressing AGREE on the Security Video screen, you will receive a Submission Successful message, including your new myCGS User ID. You will also receive a confirmation email

containing your User ID. Be sure to take note of your User ID, as you will need it every time you log in to myCGS.

11. Although your registration has now been submitted, you still need to complete your myCGS account by setting up your Multi-Factor Authentication (MFA) preferences. To do so, go to myCGS at https://mycgsportal.com, and press the ***Log In to DME myCGS*** button. Then enter your myCGS User ID and password, and press ***SUBMIT***.

12. You will be prompted to set your MFA preferences. You have the option of receiving MFA codes via text, email, or Google Authenticator. We recommend that you set up at least two forms of MFA so that you always have a backup.

    If you choose to use Text as one of your MFA options, you must enter your 10-digit cell phone number, and choose your cell phone service provider (AT&T, Sprint, T-Mobile, or Verizon).

    NOTE: If you use a cell phone carrier other than one of the four service providers listed, choose the service provider network which is used by your carrier to provide service. If you are unsure of the network, please contact your carrier. If you choose the wrong service provider, you will not receive MFA text messages.

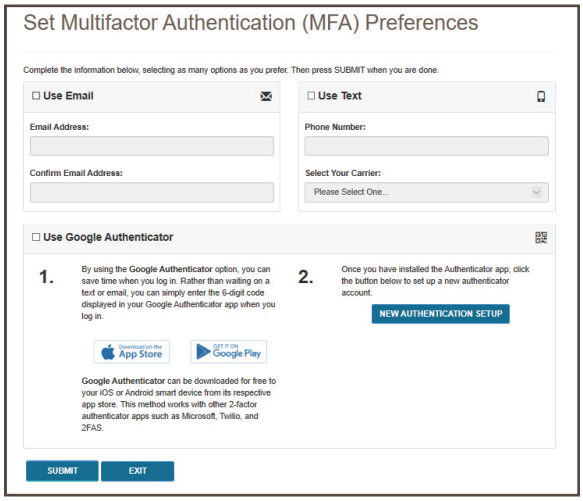
    If you choose to use Google Authenticator, you will need to either download the Google Authenticator app on your smart device (phone, tablet, etc.) or add the Google Authenticator extension to your web browser (Chrome, Firefox, or Edge). There are also third-party applications that can give you access to Google Authenticator (CGS does not provide advice on use of third-party applications). Check with your company's IT administrators to see if Google Authenticator can be made available to you and your staff.

    To use Google Authenticator, first download the appropriate app on your smart device, or download the web browser extension:

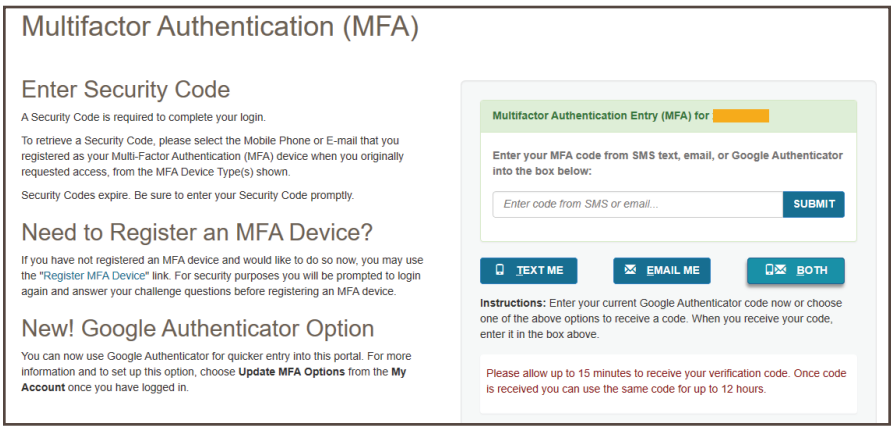
    - Apple App Store (https://apps.apple.com/us/app/google-authenticator/id388497605)
    - Google Play (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_US&gl=US)
    - Google Authenticator Browser Extension (https://authenticator.cc/)

    Then select the checkmark next to "Use Google Authenticator," or press "New Authentication Setup." A QR code will display on screen. Follow the instructions in your Google Authenticator app or web extension to scan the QR code, or manually enter the code.

    After entering your MFA information, press the ***SUBMIT*** button. If you chose Google Authenticator as one of your MFA choices, you will be immediately asked to enter your Google Authenticator code.



13. After setting up your MFA, you will immediately need to log in again and use an MFA security code to continue. On the MFA page, press the ***Text Me***, ***Email Me***, or ***Both*** button, depending on how you wish to receive your MFA security code, or if you are using Google Authenticator, simply enter your current Google Authenticator code. Note that you can use your keyboard (T for text, E for email, or B for both) to select and generate your MFA code. Once you receive the code, enter it in the MFA Code Entry field, and press ***SUBMIT*** (or press Enter on your keyboard).



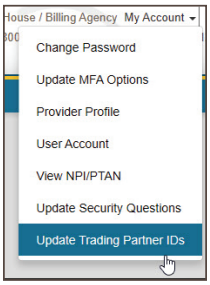
Congratulations, you have now successfully completed myCGS registration! You are now ready to use myCGS. For instructions on using myCGS to find beneficiary eligibility, claim status, and all the other great features myCGS offers, refer to the myCGS User Manual (https://www.cgsmedicare.com/jc/mycgs/pdf/mycgs_UserManual.pdf).

Update Trading Partner IDs

After you have successfully completed myCGS registration as a CHBA, you may need to add more Trading Partner IDs (for instance, if your company represents more than 10 IDs). To do so, follow the steps below.

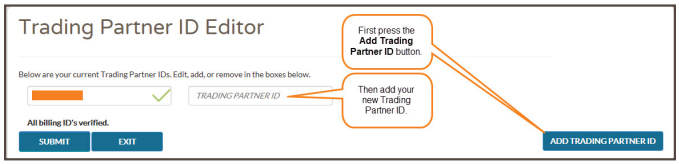
NOTE: This functionality only exists for myCGS users who are registered in the CHBA role. If you are an End User or Designated Approver, you do not have access to the Update Trading Partner IDs screen.

1. Log in to myCGS at https://mycgsportal.com.
2. In the My Account menu (found in the top-right corner of your screen), select **Update Trading Partner IDs**.



3. The Update Trading Partner IDs screen will be displayed. On this page you will see a list of your current IDs. To add a new Trading Partner ID, first press the Add Trading Partner ID button, and then enter the Trading Partner ID that you need to add to your account in the box that appears on the screen. myCGS will immediately validate whether or not the ID entered is valid and approved for CHBA use by the DMEPOS supplier. Repeat this process for each ID you need to enter.

   Once you have entered all of the appropriate Trading Partner IDs, press the ***SUBMIT*** button.



After adding your company's Trading Partner IDs, you will have access in myCGS to the NPIs/PTANs associated with each ID. Note that jurisdictional and functional permissions for each Trading Partner ID are granted by the DMEPOS supplier in their CEDI authorization agreement. If the supplier did not grant CHBAs to have access to a specific jurisdiction (B or C) or function (eligibility, claims, finance, etc.), then you will not be able to access those jurisdictions/functions in myCGS for the associated NPI/PTAN.

SECTION 2: User Management

Navigation and Options for Designated Approvers

When you log into myCGS as a Designated Approver, you are immediately taken to the User Management section of myCGS. Within User Management, you can perform the following tasks:

- Approve or deny new End User registration requests
- Recertify End Users
- Search for and view all End Users registered under your Tax ID
- Modify existing End User permissions
- Deactivate existing End Users
- Complete your annual self-recertification

Navigation

If you are in the **User Management** section of myCGS, you will see the following menu choices:

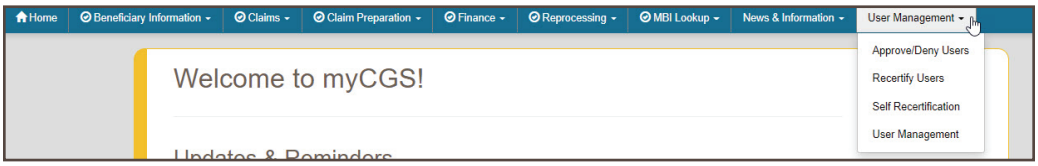
Home – The Home button will take you to the End User portion of myCGS, where you can find Eligibility, Claim Status, and all the other great features myCGS offers. For instructions, refer to the myCGS User Manual. In order to return to the User Management section of myCGS, select the My Account menu, and then choose User Management.

DA User Management – Go here to approve/deny and recertify End Users.

User Management – Go here to manage the permissions of your End Users by specific NPI/PTAN combination.

Self Recertification – Go here to complete your annual self-recertification.

If you are using the End User portion of myCGS and need to return to the User Management section, choose the appropriate screen from the User Management menu, which will be the right-most menu option on your navigation bar.



Approve/Deny Users

When a new End User submits a request to register for myCGS, the request must be approved by a Designated Approver within five days. If you are a Designated Approver (DA), you will receive an email informing you that a new request has been submitted that needs your approval. You (or another DA at your company) must log in to myCGS and approve the request before the user is granted access to myCGS.

NOTE: You must approve (or deny) End User requests within five days. If you do not take action within five days, the request will be removed and the End User will need to re-register.

To approve a user request, follow the steps below:

1. Log in to myCGS at https://mycgsportal.com.
2. As a Designated Approver, the first screen you will see when you log in is the Approve/Deny Users tab in the DA User Management screen, where any pending registration requests under your Tax ID will be shown. If you want to search for a specific user who needs to be approved/denied, enter the user's last name in the User Last Name field. Any user who matches your name search will be displayed.

The Approver/Deny Users tab will show the name, role, temporary ID, and status of End Users who have a pending registration request. Be sure to review the information of all End User request carefully before approving/denying. When you approve an End User, they will have access to your

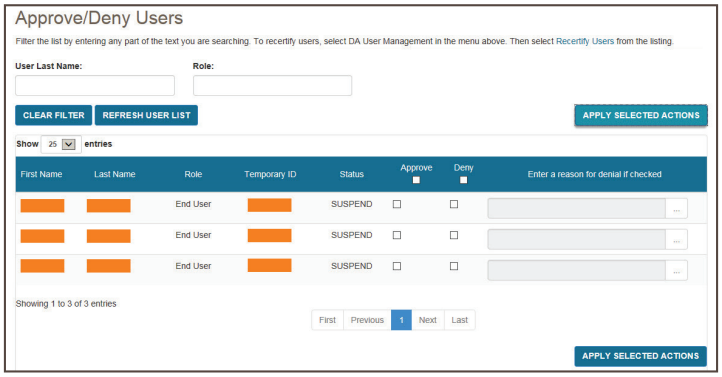
company's information (Tax ID, NPI, PTAN), such as claims submitted, check amounts, and more, in myCGS. **Only approve valid employees of your company who have a business need to use myCGS.**

To approve an End User:

- Review the user's information and ensure that they are valid employees of your company.
- Select the checkbox in the Approve field of the user's row.
- Press the **Apply Selected Actions** button.

To deny an End User:

- Select the checkbox in the Deny field of the user's row.
- Enter a reason for denial. The text you enter here will be sent to the End User via email.
- Press the **Apply Selected Actions** button.



Once you have approved or denied an End User, an email will be automatically generated and sent to the End User informing them of your approval/denial. If approved, the End User can log in and use myCGS immediately.

Recertify Users

All myCGS users must be recertified every 365 days. The recertification process ensures that myCGS access is limited to only those individuals who currently have a business need to use myCGS.

You will receive a notification email from myCGS when recertification for a user (who is registered under your company's Tax ID) is coming due. If you do not recertify the user before their certification due date, then the user will be suspended and their access to myCGS will be revoked.

To recertify users, follow these steps:

1. Log in to myCGS at https://mycgsportal.com.
2. From the DA User Management menu, select **Recertify Users**.
3. On the Recertify Users screen, your users will be shown in order of those nearest to their recertification due date, along with the following information:

   - First Name
   - Last Name
   - User ID
   - User Status
   - Days Until Certification
   - Recertification Due Date
   - Security Video Due Date

   You can use the search filters (User ID and Last Name) to search for a specific user. You can also change the order of the users displayed on screen by pressing the column header of any column. Pressing the column header a second time reverses the order (i.e., from A-Z to Z-A, etc.).

By default, myCGS displays 25 users per page. You can change the number of users displayed per page using the “Show XX entries” drop-down menu.

4. Verify whether or not the users are still active members of your organization and require myCGS access.

   To approve users for continued myCGS access, check the checkbox in the Recertify column in each user’s row. Continue to check as many users for recertification as you wish. To select all users on the page, you can use the “Select All Displayed” checkbox. Note that the select all checkbox will only select the users displayed on the current page.

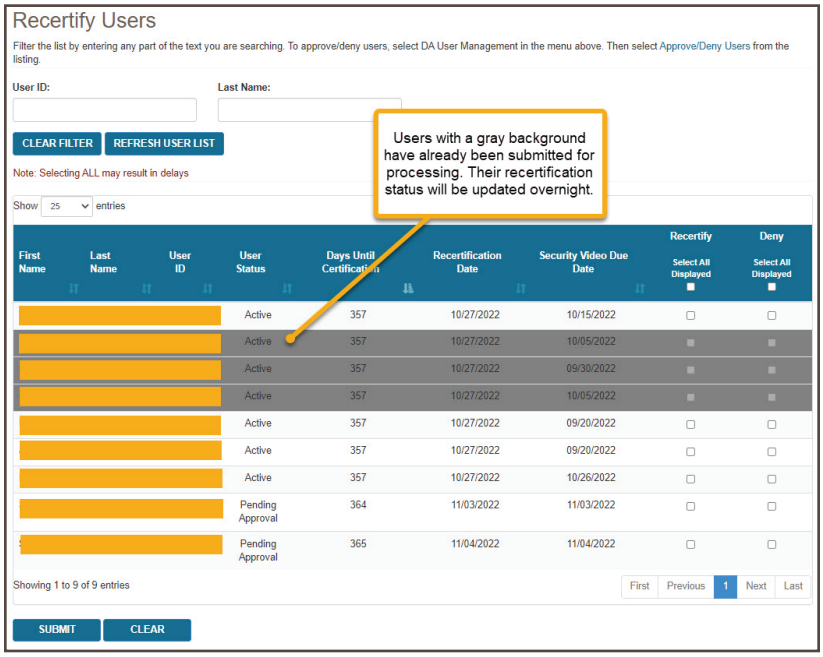
   For users who are no longer members of your organization, check the checkbox in the Deny column in each user’s row. Continue to check as many users for denial as you wish. To select all users on the page, you can use the “Select All Displayed” checkbox. Note that the select all checkbox will only select the users displayed on the current page.

   NOTE: This action will permanently disable the individual’s myCGS User ID. This action cannot be overturned. If you deny a user in error, they will need to re-register for myCGS and receive a new User ID.

   After selecting the appropriate users for recertification or denial, press the SUBMIT button. Note that you can submit users for both recertification and denial at the same time. When you press submit, all users who you’ve selected will be submitted for processing, even if you’ve selected users over multiple pages. Once submitted, your request will be processed overnight. Any users who you’ve submitted for processing will then be grayed out on the screen, as shown in the image below.

   Once recertified, the user’s recertification due date will reset to 365 days.

NOTE: If you do not recertify a user before their recertification due date, the user’s account will be suspended and their access to myCGS will be disabled until you approve their recertification.

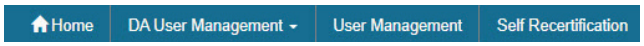


User Permissions

The User Permissions screen allows you to make changes to the user accounts of the individuals who are registered in myCGS under your company’s Tax ID. When a new user first registers for myCGS, they automatically have access to all of the NPI/PTANs associated with their approved Tax ID. If for any reason you wish to change a user’s access to certain functions or specific NPI/PTANs, then you can do so on the User Permissions screen. You can also use this screen to de-activate users who are no longer employed by your company.

NOTE: The default End User access to certain submission functions (such as Redeterminations, Reopenings, ADR, and others) is set to off. You must specifically grant access to these functions in order for your End Users to be able to use such features. Refer to the myCGS User Manual for additional information.

To access the User Permissions screen from the User Management screen of myCGS, press the **User Management** button.

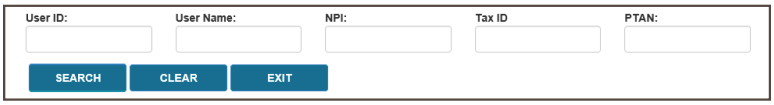


To access the User Permissions screen from the functionality section of myCGS, choose **User Management** from the User Management menu.

Searching for Users

To modify a user, first you need to search for the user. myCGS allows you to search for users by entering any of the following five pieces of user information: User ID, User Name, NPI, Tax ID, or PTAN. You can use as many of the search criterion fields as you wish.

In the User ID and User Name field, you can enter as few or as many characters as you want. For instance, if you enter “smith” in the User Name field (leaving the other fields blank), myCGS will return any user who has “smith” in their name, be it Jill Smith, Stan Smith, Karen Smithson, or Smith Jones.



Once you have entered the appropriate search criteria, press the ***SEARCH*** button.

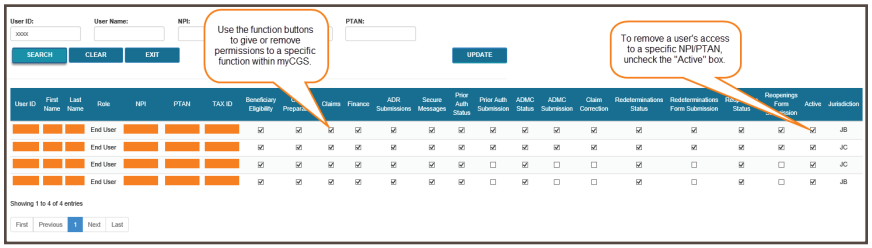
Modifying Users

After performing your search, myCGS will display the profile information for any users who match your search criteria. Note that if you have more than one NPI/PTAN, multiple rows may exist for a single user who shares the same multiple NPI/PTAN information. Changes made to user permissions are made on an individual NPI/PTAN basis.

To add or remove permissions to a function screen within myCGS, check or uncheck the appropriate checkbox (a check means the user has permission to use the function screen; unchecked means they are not permitted to use the screen).

To de-activate a user entirely from myCGS, check the Deny checkbox and enter a rejection reason in the text field.

Once you have made the appropriate changes to the user’s profile, press the ***UPDATE*** button.



Self Recertification

All myCGS users must be recertified every 365 days. The recertification process ensures that myCGS access is limited to only those individuals who currently have a business need to use myCGS. As a DA, you are responsible for recertifying your End Users (see the Recertify Users section above). For your own recertification, you must complete a self-recertification in myCGS using the Self Recertification screen.

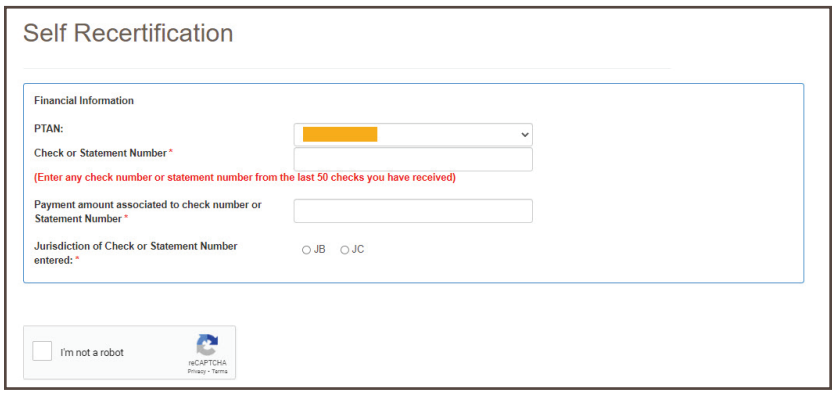
When your self-recertification is coming due, you will receive email notifications to let you know when your self-recertification must be completed by. You will also receive messages when you log in to myCGS asking you to complete your self-recertification.

To access the Self Recertification screen from the User Management screen of myCGS, press the ***Self Recertification*** tab.

To access the Self Recertification screen from the functionality section of myCGS, choose **Self Recertification** from the User Management menu.

To complete your self-recertification, enter the check/EFT number or statement number and dollar amount of one the 50 most recent checks issued to your company by CGS DME MAC Jurisdiction B or C in the "Check or Statement Number" and "Payment amount associated to check number or statement number" fields. Also select the Jurisdiction (JB or JC) of the check. The check must match the PTAN displayed on the page. If you have more than one PTAN, you can select any of your PTANs from the PTAN drop-down menu, and then enter matching check information. Once you've entered your check information, complete the reCAPTCHA field, and then press the ***SUBMIT*** button to complete your recertification.

NOTE: Once you've completed the reCAPTCHA field, you must press the SUBMIT button within one minute or else the verification will expire. If the reCAPTCHA verification does expire, simply complete the field again and then press SUBMIT.



Adding Additional Tax IDs

myCGS registration is based around a supplier's Tax ID. All NPI/PTAN combinations that are associated with your Tax ID are automatically added to your myCGS account upon successful registration. Some suppliers, however, may have multiple Tax IDs, with different NPI/PTAN combinations under each Tax ID. If your company has more than one Tax ID, then your Authorized Official (AO) or Delegated Official (DO) will need to assign the additional Tax ID to the existing Designated Approver (DA). To do so, the AO/DO must complete the myCGS Additional Tax ID Request Form, which is found on our website at https://www.cgsmedicare.com/jc/forms/pdf/mycgs_additional_tax_id.pdf. The completed and signed form must be faxed to us at 1.615.664.5994.

NOTE: If you do not have the ability to fax, you can mail your form to CGS, ATTN: myCGS Registration, PO Box 20010, Nashville, TN 37202

Once we have processed the form, we will add the additional Tax ID to the DA's myCGS profile and will be available within 5 to 10 business days. In doing so, all End Users who have previously been approved by the DA will also receive access to the additional Tax ID (and all associated NPI/PTAN combinations) automatically.

SECTION 3: Security and Account Maintenance

Passwords

Passwords are an important part of securing both beneficiary data and your company's data. Your myCGS password should be kept up to date (changed every 60 days) and should be known only to you. Your ID will be disabled if you do not log in for 30 consecutive days. Your account will be locked if you enter your password incorrectly three consecutive times within a 120-minute period.

NOTE: In order to qualify as an active login, you must successfully complete the entire myCGS login process, including use of your MFA code. If you do not log in for 30 consecutive days, your account will be suspended—in order to reactivate your account, you must call our Provider Contact Center (Jurisdiction B: 1.866.590.6727, Jurisdiction C: 1.866.270.4909). If you do not log in for 90 consecutive days, your account will be deactivated, and you will need to re-register for myCGS.

myCGS keeps count of consecutive invalid login attempts within a 120-minute period until there is a successful login. Once your account is locked, you must call our Provider Contact Center in order to have your account unlocked. We recommend that if you have two consecutive unsuccessful login attempts that you do one of the following to prevent being locked out:

- Wait 120 minutes and then try to log in again **OR**
- Use the "Forgot Password" link on the login screen to reset your password

Passwords in myCGS must:

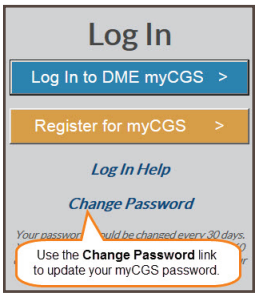
- Be at least eight characters
- Begin with a letter
- Include at least one upper case letter
- Include at least one lower case letter
- Include at least one number
- Include at least one special character (such as @,#, $, etc.)
- Contain at least six different characters than your previous password
- May not be the same as one of your previous 12 passwords

When you change your password, you cannot reuse any of your previous 12 passwords. Additionally, your new password must contain at least six different characters than your previous password, or if you reuse the same characters, they must be in a different position in the password. For example, if your previous password started with the letter P, your new password should start with a different character, but you can still use the letter P in a different position of the password.

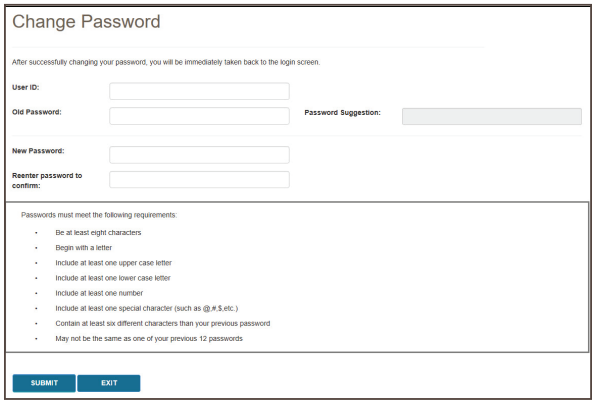
Example: Your old password is Portal$84. If you attempt to change to a new password of Portal#92, myCGS will give you an error message stating that you need to use different characters for your password. This is due to the fact that six characters ("Portal") are the same characters in the same position as your previous password. If you instead change your password to Latrop#92, this password would be accepted because even though six of the same characters are reused, they are in different positions.

Change Password

To change your myCGS password, use the ***Change Password*** link found on the initial myCGS "splash" page (before you log in) or if you're already logged in, select the Change Password option in the My Account menu.



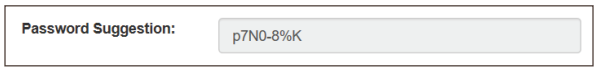
On the Change Password screen, enter your myCGS User ID and previous (old) password, and then enter your new password twice. Note that myCGS includes an optional suggested password in case you are having difficulty creating your own password (see the Password Suggestion section below). Press the ***SUBMIT*** button to complete your password change.



Password Suggestion

When changing your password, myCGS offers an optional "password suggestion" that you can use as your new password. To use the password suggestion, follow these steps:

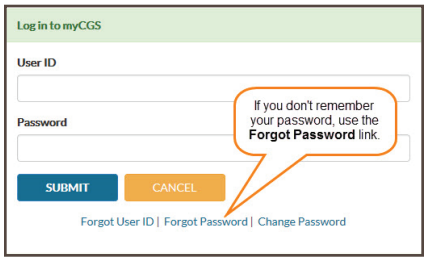
1. Go to the Change Password screen in myCGS.
2. Enter your User ID. (The suggested password will not appear unless you have done this step.)
3. Type the suggestion into the New Password field, re-enter to confirm, and press SUBMIT. For security reasons, you cannot copy and paste the password suggestion.



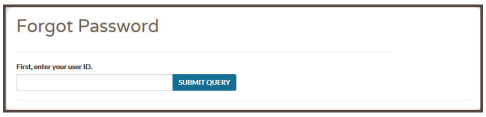
Forgot Password

If you don't remember your myCGS password and need to have it reset, follow these steps:

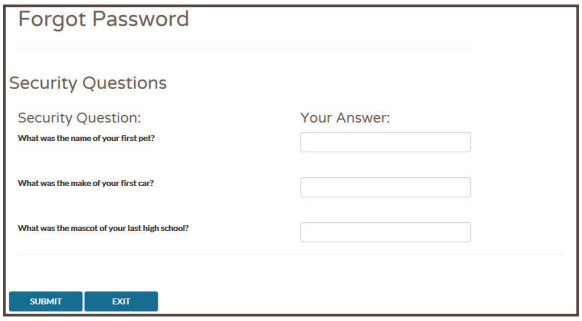
1. Go to myCGS (https://mycgsportal.com), and press the **Log In to myCGS** button.
2. On the login screen, press the ***Forgot Password?*** link.



3. You will be prompted to enter your User ID. Enter your ID, and press ***Next***.

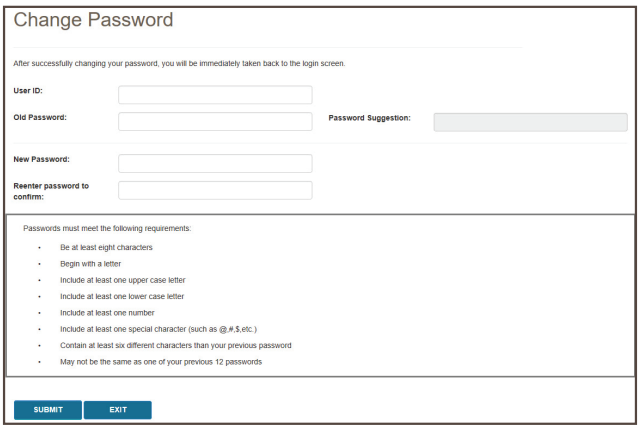


4. Next you will need to answer your security challenge questions. Enter the answers to all three questions, and press ***SUBMIT***.



5. After answering the questions correctly, you will receive an email containing a link to reset your password. Once you receive the email, follow the password reset link. This will take you to the Change Password screen in myCGS.

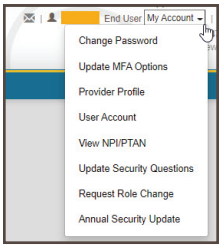
6. On the Change Password screen, enter your User ID (which was provided via email), and select a password using either the optional Password Suggestion shown on the screen or a password of your own creation. Once you have confirmed the password, press ***SUBMIT*** to complete your password change.



User Account

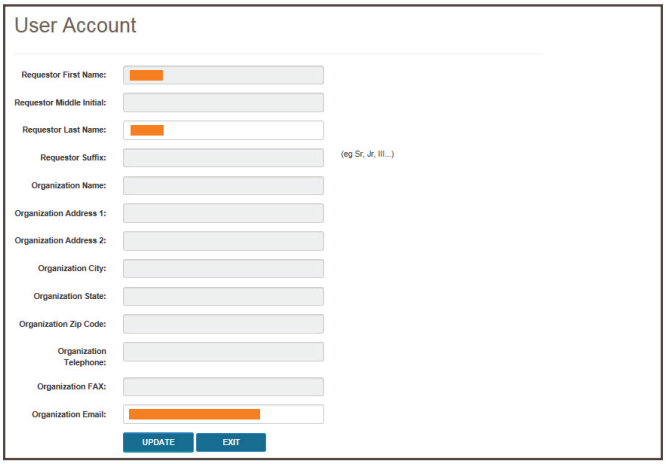
The User Account screen allows you to update your last name and email address. It is important to keep your email address up to date so that we can contact you with important messages about myCGS, including password resets.

To access the User Account screen, select the ***User Account*** option in the My Account menu (found in the top-right corner of the screen).



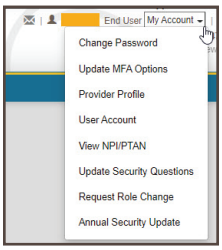
On the User Account screen, you can update your last name and/or email address using the available text boxes. Make your changes, and press the ***UPDATE*** button.

NOTE: The email address listed under User Account is separate from the email address listed in your MFA settings. Changing the email address your User Account does not affect the email address in your MFA settings (and vice versa). If your email address has changed, you must update it on both screens. Refer to the ***Update Your MFA Settings*** section below.



Update MFA Options

If you need to update or change your cell phone, email information, or Google Authenticator account that is associated with your Multi-Factor Authentication (MFA) settings, go to the MFA Options screen. To access the MFA Options screen, select the My Account menu found in the top-right corner of your screen, and choose Update MFA Options.



On the MFA Options screen, you can add or alter your MFA email address, cell phone information, and/or Google Authenticator. We recommend that you set up at least two forms of MFA so that you always have a backup.

If you choose to use Text as one of your MFA options, you must enter your 10-digit cell phone number, and choose your cell phone service provider (AT&T, Sprint, T-Mobile, or Verizon).

NOTE: If you change cell phone carriers, you must update your Service Provider to reflect your current carrier in order to continue to receive myCGS MFA text messages, even if your cell phone number remains unchanged. If you use a cell phone carrier other than one of the four service providers listed, choose the service provider network which is used by your carrier to provide service. If you are unsure of the network, please contact your carrier. If you choose the wrong service provider, you will not receive MFA text messages.

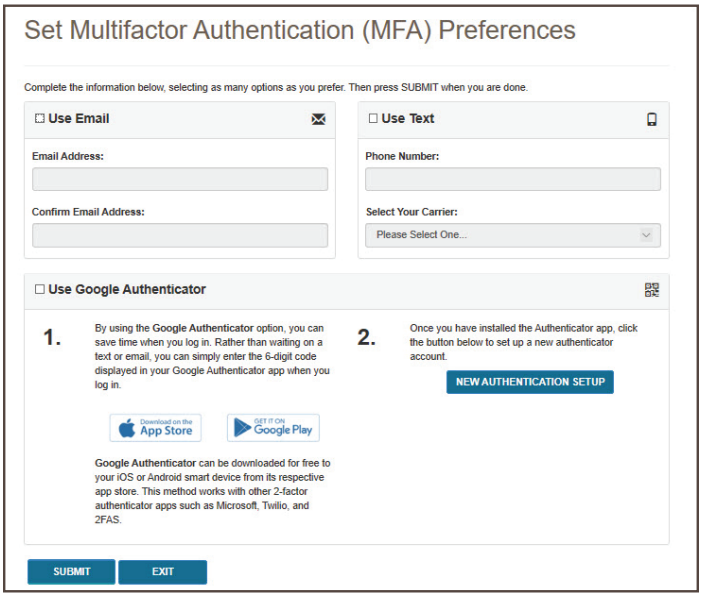
If you choose to use Google Authenticator, you will need to either download the Google Authenticator app on your smart device (phone, tablet, etc.) or add the Google Authenticator extension to your Web browser (Chrome, Firefox, or Edge). There are also third-party applications that can give you access to Google Authenticator (CGS does not provide advice on use of third-party applications). Check with your management to see if Google Authenticator can be made available to you.

To use Google Authenticator, first download the appropriate app on your smart device, or download the Web browser extension:

- Apple App Store: https://apps.apple.com/us/app/google-authenticator/id388497605
- Google Play: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_US&gl=US
- Google Authenticator Browser Extension: https://authenticator.cc/

Then select the checkmark next to “Use Google Authenticator,” or press “New Authentication Setup.” A QR code will display on screen. Follow the instructions in your Google Authenticator app or Web extension to scan the QR code, or manually enter the code.

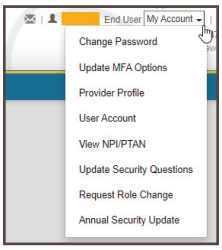
NOTE: You must press ***SUBMIT*** in myCGS in order for your account to be saved and linked to your Google Authenticator app.



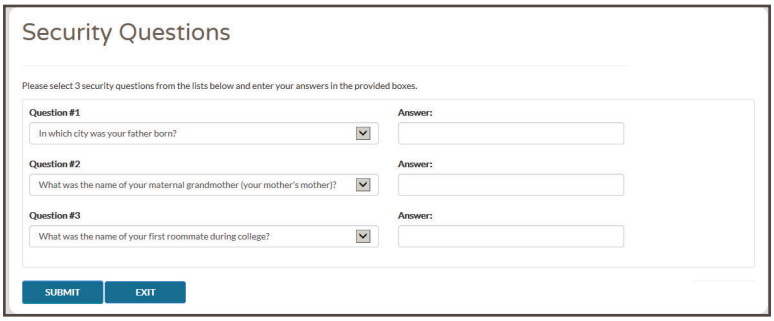
Make any necessary changes to your information, and press the ***SUBMIT*** button. If you chose Google Authenticator as one of your MFA choices, you will be immediately asked to enter your Google Authenticator code.

Update Security Challenge Questions & Answers

If you wish to update or change your security challenge questions and answers, go to the Update Security Questions screen. To access the Security Questions screen, select the **My Account** menu found in the top-right corner of your screen, and choose **Update Security Questions**.



Choose questions from each of the three drop-down menus, and answer them accurately. Be sure to choose questions and answers that are personal to you and that you will remember. You will need to be able to answer the challenge questions should you forget your password and need to have it reset.

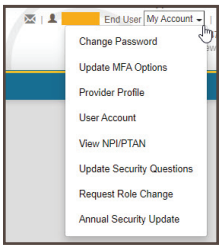


For further information about myCGS, refer to the User Manual (https://www.cgsmedicare.com/jc/mycgs/pdf/mycgs_UserManual.pdf).

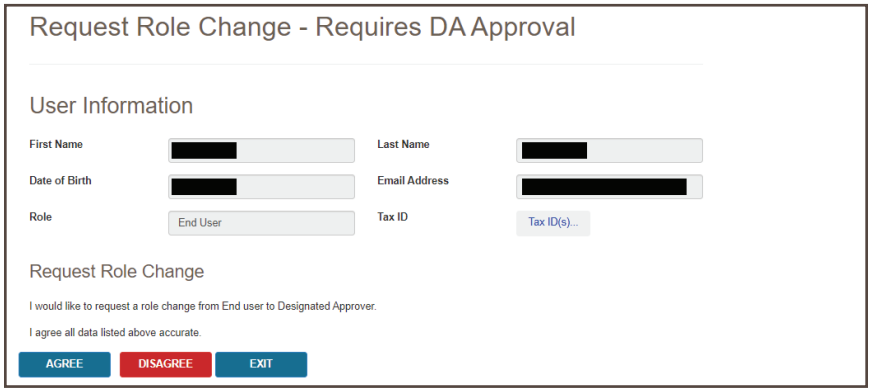
Request Role Change

myCGS allows for registered End Users to request that their role be changed to become a Designated Approver (DA). If you are registered in myCGS as an End User and need to be promoted to a DA, select the **My Account** menu found in the top-right corner of your screen, and choose **Request Role Change**.

NOTE: There must be an active DA from your company currently registered in myCGS in order to approve the role change. If there is no active DA, then a new DA must successfully complete registration before a role change can be made.



On the Request Role Change screen, ensure that your information is correctly listed, and then press the Agree button. Your role change request will then be sent to your Designated Approver for approval (or denial).



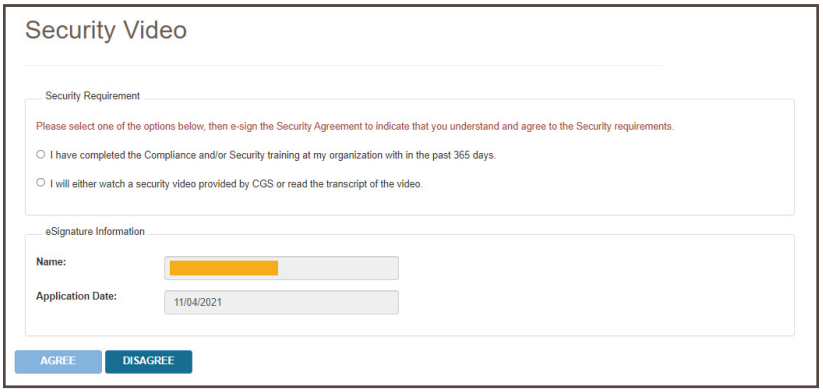
Once your current Designed Approver approves your role change request, you will have full Designated Approver access. Note that your company may have multiple Designed Approvers in myCGS (there is no limit).

Annual Security Update

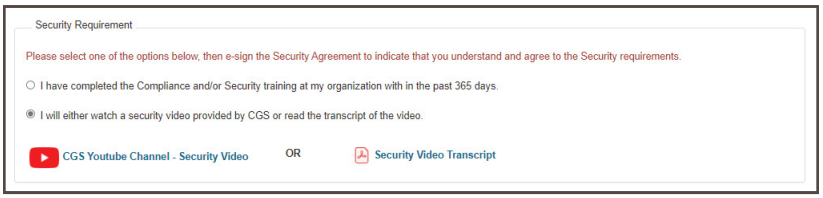
CGS requires that all myCGS users complete annual compliance/security training in order to ensure that our users are familiar with best practices related to protecting both beneficiary and supplier information, as well as your own personal information. When your annual compliance/security training is coming due, you will receive email notifications to let you know when the security update must be completed by. You will also receive messages when you log in to myCGS asking you to complete your annual security training.

To complete your annual security update, follow these steps:

1. Log in to myCGS. If your security update is due soon, you will receive a message asking if you wish to complete the security update. Press the ***BEGIN*** button. You can also access the Annual Security Update via the **My Account** menu found in the top-right corner of your screen, and choosing **Annual Security Update**.
2. You will be taken to the Terms of Use screen. Your name and today's date will automatically populate in the eSignature Information section at the bottom of the page. Read the terms of use carefully. If you agree to the terms of use, press the AGREE button. Note that you must agree to the terms of use in order to continue to use myCGS.
3. You will then be taken to the Security Video screen. If your company provides annual compliance/security training which you have taken within the past 365 days, then choose the first option on the screen and press the AGREE button.



If you have not received any compliance/security training within the past 365 days, then select the second option. This will present you with the option of either watching a security video provided by CGS or reading the transcript of the video. Note that the security video is approximately 12 minutes in length.



After you have either watched the video or read the video transcript, press the AGREE button. Note that you must agree to complete annual compliance/security training in order to continue to use myCGS.