

interChange Provider Important Message

Attention: All Providers, Trading Partners and Drug Labelers

Multi-Factor Authentication (MFA) Is Mandated Effective August 1, 2026, Open Office Hours for Multi-Factor Authentication /Security Questions

1. Office Hours Available for Security and Multi-Factor Authentication Questions:

Gainwell Technologies will be hosting open Office Hours where you can meet with a Gainwell representative to ask questions you may have about Security and Multi-Factor Authentication. Please join us during the following dates and times. Register by clicking the links below for your desired date.

Once registered, providers will be presented with a confirmation page containing the link to join the Office Hours for the date and time selected. Please copy and paste the link to your calendar. Additionally, a meeting reminder will be sent to the email address used in registration the day before the meeting.

[August 3, 2026: 9 am to 10 am](#)

[August 4, 2026: 12 pm to 1 pm](#)

[August 5, 2026: 3 pm to 4 pm](#)

[August 6, 2026: 10:30 am to 11:30 am](#)

[August 7, 2026: 9 am to 10 am](#)

More to be scheduled.

2. Secure Web Portal Multi-Factor Authentication (MFA) Enrollment for Master Users and Clerks mandated use by August 1, 2026

The Connecticut Medical Assistance Program's (CMAP) secure Web Portal introduced **Multi-Factor Authentication (MFA)** to enhance security for Master Users and Clerks on June 2, 2026. MFA will no longer be optional as of August 1, 2026. All Providers, Trading Partners and Drug Labelers will be required to enroll with MFA on August 1, 2026.

Since Tuesday, June 2, users have seen an MFA enrollment screen upon login. Users have two options, using an Authenticator App (downloaded to one device of your choice) or Email Verification. Users may opt to enroll with one or both methods, and choose their preferred option each time they log in. Enrollment may be bypassed until August 1, 2026 by clicking on the Skip for Now button.

Screen Example:



interChange Provider Important Message

Multi-Factor Authentication Enrollment

Protect your account with an extra layer of security by enrolling in Multi-Factor Authentication (MFA). MFA adds an additional verification step to confirm your identity, helping prevent unauthorized access even if your password is compromised.

Once enrolled, you will be required to verify your identity when performing the following actions:

- Logging in to your account
- Changing your password
- Resetting your password
- Updating Electronic Funds Transfer (EFT) information

Enrolling in MFA is a simple and effective way to protect your personal and financial information and keep your account secure.

Verification Method	Status	Action
Authenticator App (TOTP) Microsoft Authenticator, Google Authenticator, or any compatible app. One device supported.	Not Enrolled	Set Up
Email Verification (OTP) One-time code sent to your registered email. One registration per account.	Not Enrolled	Set Up

📞 **Having trouble?** If you are unable to complete verification, ask your **Master User** to remove your MFA enrollment so you can re-enroll. If you are the Master User, call the **Provider Assistance Center at 1-800-842-8440** (Mon-Fri, 8:00 am-5:00 pm) to have your MFA reset.

Option 1: Authenticator App

Users may set up MFA using an authenticator application downloaded to their mobile device for free from the Google Play store (Android) or the Apple App Store (iPhone/iPad) or they may decide to enroll with **E-mail Verification** which is outlined in the next section.

Recommended applications include (this is the user's choice):

- Microsoft Authenticator
- Google Authenticator
- Authy Authenticator
- RFC 6238 compatible application

During Setup - after clicking Set Up button:

- Install an Authenticator App of your choice on your device.
- The screen will display a **QR code** and a **manual entry key**
- Scan the QR code with your authenticator app
- Device Name - name your device and select which Authenticator App you are using.
- Enter the generated **6-digit code**
- Select **Verify & Enroll Device**

interChange Provider Important Message

ne Information Provider Trading Partner Pharmacy Information Hospital Modernization Telehealth Information

ctronic Visit Verification Claims Eligibility Prior Authorization Hospice **Account**

home account home account maintenance account setup change password document upload reset password **mfa enrollment**

og out

Multi-Factor Authentication Enrollment

Set Up Authenticator App

1

Install an authenticator app on your mobile device

If you don't already have one, download and install a free authenticator app from your device's app store:

- **Microsoft Authenticator** — recommended for Windows/Microsoft users
- **Google Authenticator** — simple and widely used
- **Authy** — supports backup and multiple devices

Search for the app name in the **Apple App Store** (iPhone) or **Google Play Store** (Android), then tap **Install**. Once installed, open the app and follow the initial setup prompts if any.

2

Scan the QR code below using your authenticator app

In your authenticator app, tap the + (add account) button, then select "Scan a QR code". Point your phone's camera at the QR code shown below. The app will automatically add an entry labeled "CT Medicaid Portal" and begin generating 6-digit codes that refresh every 30 seconds.



Can't scan? Enter this key manually in your app:

In your app, choose "Enter a setup key" instead of scanning. Type the key above exactly as shown (spaces are optional). Select **Time-based** when asked.

3

Name this device and select your app

Give this device a name you'll recognize later (e.g., "My iPhone" or "Work Android").

Device Name *

e.g. My iPhone, Work Android

Required — helps identify this device later.

Authenticator App

-- Select App --

4

Enter the 6-digit code from your app to verify setup

Look at your authenticator app — you should see a 6-digit number under "CT Medicaid Portal" that changes every 30 seconds. Type the current code into the field below and click **Verify & Enroll Device**. If the code has almost expired (timer nearly at zero), wait for the next code.

Verification Code

Verify & Enroll Device

Cancel

ⓘ **Having trouble?** If you are unable to complete verification, ask your **Master User** to remove your MFA enrollment so you can re-enroll. If you are the Master User, call the **Provider Assistance Center at 1-800-842-8440** (Mon–Fri, 8:00 am–5:00 pm) to have your MFA reset.

NOTE: If a user has skipped the MFA enrollment or needs to make an enrollment change, they can access the enrollment screen by going on the **Account** tab and select **MFA enrollment**.

interChange Provider Important Message

Home	Information	Provider	Trading Partner	Pharmacy Information	Hospital Modernization	Telehealth Information
Electronic Visit Verification	Claims	Eligibility	Prior Authorization	Hospice	Account	
home	account home	account maintenance	account setup	change password	document upload	reset password
log out						mfa enrollment

- Once Enrolled you will be able remove a device after logging in by clicking on the **Remove All** button.

Multi-Factor Authentication Enrollment

Protect your account with an extra layer of security by enrolling in Multi-Factor Authentication (MFA). MFA adds an additional verification step to confirm your identity, helping prevent unauthorized access even if your password is compromised.

Once enrolled, you will be required to verify your identity when performing the following actions:

- Logging in to your account
- Changing your password
- Resetting your password
- Updating Electronic Funds Transfer (EFT) information

Enrolling in MFA is a simple and effective way to protect your personal and financial information and keep your account secure.

Verification Method	Status	Action
Authenticator App (TOTP) Microsoft Authenticator, Google Authenticator, or any compatible app. One device supported.	✓ Enrolled	Remove All Maximum of 1 device allowed. Remove a device to add a new one.
Email Verification (OTP) One-time code sent to your registered email. One registration per account.	Not Enrolled	Set Up

Enrolled Devices

Device Name	App	Enrolled Date	Status	Action
Iphone 2	Microsoft Authenticator	06/22/2026	Active	Remove

Last 10 Activities

Activity	Method	Operation	Date	Details / Device
				Email

interChange Provider Important Message

Option 2: E-mail Verification

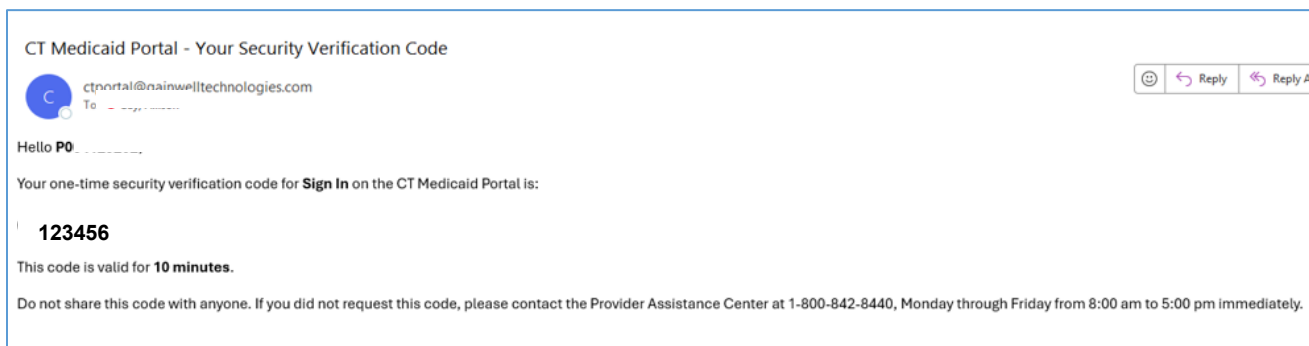
During Setup - after clicking Set Up button:

- Validate that you have a current email address showing on this screen.
- If the email is out of date, update your email under Account tab, select Account Maintenance.
- A verification code will be sent to your registered e-mail address
- Enter the **6-digit code** received via e-mail
- Select **Verify & Enroll** to complete the process

The top screenshot shows a 'Security Verification' window with the text: 'Click to send a 6-digit code to your registered email address: [email address]@gainwelltechnologies.com'. Below this is a button labeled 'Send New Verification Code'.

The bottom screenshot shows the same window after the code has been sent. It displays the message: 'A 6-digit code will be sent to your registered email address.' and 'A verification code has been sent to your registered email address.' Below this is another 'Send New Verification Code' button. Further down, it says 'Enter Verification Code' and shows the code '123456' in a text box. At the bottom are 'Verify' and 'Cancel' buttons.

Example of email sent:



Note: The Email verification code is only valid for **10 minutes**, after that you will need to select **Send New Verification Code** again.

Not receiving the email? Check your spam or junk folder. To ensure reliable delivery, add @gainwelltechnologies.com to your safe senders (allowlist) in your email application.

Having trouble? If you are unable to complete verification, ask your Master User to remove your MFA enrollment so you can re-enroll. If you are the Master User,

interChange Provider Important Message

call the Provider Assistance Center at 1-800-842-8440 (Mon-Fri, 8:00 am-5:00 pm) to have your MFA reset.

Multi-Factor Authentication Enrollment

Protect your account with an extra layer of security by enrolling in Multi-Factor Authentication (MFA). MFA adds an additional verification step to confirm your identity, helping prevent unauthorized access even if your password is compromised.

Once enrolled, you will be required to verify your identity when performing the following actions:

- Logging in to your account
- Changing your password
- Resetting your password
- Updating Electronic Funds Transfer (EFT) information

Enrolling in MFA is a simple and effective way to protect your personal and financial information and keep your account secure.

Verification Method	Status	Action
Authenticator App (TOTP) Microsoft Authenticator, Google Authenticator, or any compatible app. One device supported.	✓ Enrolled	Remove All Maximum of 1 device allowed. Remove a device to add a new one.
Email Verification (OTP) One-time code sent to your registered email. One registration per account.	✓ Enrolled Email: hppro@ologies.com	De-register

Enrolled Devices

Device Name	App	Enrolled Date	Status	Action
iPhone 2	Microsoft Authenticator	06/22/2026	Active	Remove

Last 10 Activities

Once enrolled with MFA you will be required to use this authentication for the following actions:

- Logging into the portal
- Changing/resetting passwords
- Updating electronic fund transfer (EFT) information

For questions, please contact the Provider Assistance Center, Monday through Friday from 8:00 a.m. to 5:00 p.m. at 1-800-842-8440 or [please join our upcoming office hours which will be scheduled weekly.](#)

3. Web Portal Security Question and Notification Changes effective May 13, 2026

The Connecticut Medical Assistance Program (CMAP) secure Web Portal made a change in security question structure and change notification. When a user needs to reset a password, Master Users/local administrators and clerks are required to select two (2) security questions from a structured list of questions utilizing a drop-down menu and entering corresponding answers to these questions, this replaces free form questions effective May 13, 2026.

interChange Provider Important Message

Master Users/local administrators and clerks also have the ability after May 13, 2026 to reset their own security questions and answers using the new structure by accessing Account Maintenance within their secure Web Portal. Go to Account and select Account Maintenance. Questions and answers may be modified using the drop-down structured questions.

The screenshot shows the 'Account Maintenance' page of a web portal. At the top, there is a navigation bar with links: Home, Information, Provider, Trading Partner, Pharmacy Information, Hospital Modernization, Telehealth Information, Electronic Visit Verification, Claims, Eligibility, Prior Authorization, Trade Files, Messages, Behavioral Health Attestation, and Account (highlighted in red). Below this is a sub-navigation bar with links: home, account home, account maintenance (highlighted in red), account setup, change password, document upload, reset password, and switch provider. A 'log out' link is also present. The main content area is titled 'Account Maintenance' and contains two sections: 'User Profile' and 'Security Questions'. The 'User Profile' section includes fields for User ID (CLERKTEST30), Contact First Name* (Joe), Contact Last Name* (Test), Phone Number* (two input boxes), Email* (one input box), Confirm Email* (one input box), and AVR ID (one input box). The 'Security Questions' section includes two sets of dropdown menus for '1st Secret Question*' and '1st Answer*', and '2nd Secret Question*' and '2nd Answer*'. At the bottom right, there are four buttons: 'save', 'cancel', 'change password', and 'reset AVR Pin'.

Once a password, contact information or security questions are updated a user and/or their Master User will receive the following message:

Dear [USER ID NAME]

The security information associated with the Connecticut Medical Assistance Program's Secure Web portal account for user ID [USER ID NAME] has changed.

If you did not initiate this change and you are a Master User, please contact the Provider Assistance Center at 1-800-842-8440, Monday through Friday from 8:00 am to 5:00 pm. If you are a Drug Manufacturer, please email ctdrugrebate@gainwelltechnologies.com. If you are a clerk, please contact the Master User for your organization.

Thank you,

Connecticut Medical Assistance Program

Security Reminders:

Every 60 days, Master Users/local administrators and clerks are prompted to change their password. Users enter their existing password, their new password, and then are asked to confirm this new password. If the new passwords does not match, the user is given a "New Password must be same as Confirm New Password" error message. Users may not re-use any of their last 6 passwords.

Password Requirements:



interChange Provider Important Message

- The Password you enter must be **15 - 30 characters** in length. The Password and Confirm Password fields must match exactly. The password must have **at least 3 of the 4 character types** - upper case, lower case, number, special character. Special characters include such characters as the following: # \$ % ^ @ *
- Both Secret Question and Answer fields are required. Questions are selected from the drop-down menu. Answers should not contain any special characters, only upper- and lower-case alpha, 0-9 numeric characters, and blank spaces are permitted.

Users have the ability to make **4 attempts** to enter the correct ID / password or two security question / answer combinations before the account is locked.

Please correct the following errors:

We are sorry but the user name or password is incorrect. Your account will be locked after 4 invalid attempts. Please try again.

After 4 attempts you will receive the following message:

Your account has been locked due to too many invalid password attempts. **Please select the reset password button to answer security questions and unlock your account.** If you are a Master User that is unable to use the reset password service, please contact the Provider Assistance Center at 1-800-842-8440. If you are a Drug Manufacturer, please email CTDrugRebate@gainwelltechnologies.com. If you are a Clerk, please contact the Master User for your organization.

Master Users are able to UNLOCK clerk IDs through the portal.

If the Master User/local administrator or clerk does not use their ID and password for 90 days, their user account is disabled. The local administrator and/or clerk should follow the self-service instructions on the Secure Web site log in page to reactivate their account. The provider or trading partner's Master User/local administrator should only contact the Provider Assistance Center for help at 1-800-842-8440 if panel messages indicate that an account is in a locked/disabled status where there is no longer any self-service functionality available. If the local administrator is a labeler/drug manufacturer, an email should be sent to ctdrugrebate@gainwelltechnologies.com.

IMPORTANT: If a clerk is not able to use the self-service functionality, they should contact the Master User/local administrator of their organization to reset their password.



interChange Provider Important Message

REMEMBER: User IDs and passwords must always be safeguarded and should never be shared.

Additional instructions on Web Portal set up as well as ongoing account maintenance can be found on the www.ctdssmap.com Web site, under Information > Publications > Chapter 10 Web Portal/AVRS > Web Security Administration.

For questions, please contact the Provider Assistance Center, Monday through Friday from 8:00 a.m. to 5:00 p.m. at 1-800-842-8440. If you are a Drug Manufacturer, please email ctdrugrebate@gainwelltechnologies.com.