



FollowMyHealth®

FollowMyHealth Support for Managing Two-Factor Authentication and Trusted Devices

Published Date: January 18, 2024 for release of FollowMyHealth®
For further information about this manual or other Veradigm LLC products, contact Global Service Center.

Global Service Center

Client Portal Website: <https://central.allscripts.com> (Client Portal login is required. Contact information varies by product.)

Contact us: <https://veradigm.com/contact/>

Proprietary Notice

© 2024 Veradigm LLC and/or its affiliates. All rights reserved.

This document contains confidential and proprietary information protected by trade secret and copyright law. This document, the information in this document, and all rights thereto are the sole and exclusive property of Veradigm LLC and/or its affiliates, are intended for use by customers and employees of Veradigm LLC and/or its affiliates and others authorized in writing by Veradigm LLC and/or its affiliates, and are not to be copied, used, or disclosed to anyone else, in whole or in part, without the express written permission of Veradigm LLC and/or its affiliates. For authorization from Veradigm LLC to copy this information, please call Veradigm Global Service Center at 888 GET-HELP or 888 438-4357. Notice to U.S. Government Users: This is "Commercial Computer Software Documentation" within the meaning of FAR Part 12.212 (October 1995), DFARS Part 227.7202 (June 1995) and DFARS 252.227-7014 (a) (June 1995). All use, modification, reproduction, release, performance, display, and disclosure shall be in strict accordance with the license terms of Veradigm LLC and/or its affiliates. Manufacturer is Veradigm LLC, and/or its affiliates, 222 Merchandise Mart Plaza, Suite #2024, Chicago, IL 60654.

IMPORTANT NOTICE REGARDING GOVERNMENT USE

The software and other materials provided to you by Veradigm LLC include "commercial computer software" and related documentation within the meaning of Federal Acquisition Regulation 2.101, 12.212, and 27.405-3 and Defense Federal Acquisition Regulation Supplement 227.7202 and 52.227-7014(a). These materials are highly proprietary to Veradigm LLC and its vendors. Users, including those that are representatives of the U.S. Government or any other government body, are permitted to use these materials only as expressly authorized in the applicable written agreement between Veradigm LLC and your organization. Neither your organization nor any government body shall receive any ownership, license, or other rights other than those expressly set forth in that agreement, irrespective of (a) whether your organization is an agency, agent, or other instrumentality of the U.S. Government or any other government body, (b) whether your organization is entering into or performing under the agreement in support of a U.S. Government or any other government agreement or utilizing any U.S. Government or any other government funding of any nature, or (c) anything else.

FollowMyHealth® is a trademark of Veradigm LLC and/or its affiliates.

Cited marks are the property of Veradigm LLC and/or its affiliates. All other product or company names are the property of their respective holders, all rights reserved.

The names and associated patient data used in this documentation are fictional and do not represent any real person living or otherwise. Any similarities to actual people are coincidental.

Images and option names used in this documentation might differ from how they are displayed in your environment. Certain options and labels vary according to your specific configuration. Images are for illustration purposes only.

Fee schedules, relative value units, conversion factors and/or related components are not assigned by the AMA, are not part of CPT, and the AMA is not recommending their use. The AMA does not directly or indirectly practice medicine or dispense medical services. The AMA assumes no liability for data contained or not contained herein.

Excel, Microsoft, and BizTalk are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe, the Adobe logo, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

iPhone® and iPad® are trademarks of Apple Inc., registered in the U.S. and other countries.

Perceptive Content, Lexmark, and the Lexmark logo are trademarks of Lexmark International, Inc., registered in the United States and/or other countries.

InterQual and InterQual Connect are registered trademarks of Change Healthcare, LLC in the United States or other countries.

Table of contents

Overview.....	5
FollowMyHealth Dashboard Users.....	7
Managing two-factor authentication.....	7
Resetting two-factor authentication.....	12
Managing trusted devices.....	15
Personal Health Record Users.....	19
Managing sign-in preferences.....	19
Add two-factor authentication to your account.....	19
Change two-factor authentication to your account.....	21
Turn off two-factor authentication.....	23
Signing in with two-factor authentication.....	23

Overview

To support the FollowMyHealth Quarterly Attestation for 2015 CURES, the following information summarizes the support for managing two-factor authentication in both the FollowMyHealth Dashboard and in the FollowMyHealth Personal Health Record, and managing trusted devices in the FollowMyhealth Dashboard.



Overview

FollowMyHealth Dashboard Users

Managing two-factor authentication

The FollowMyHealth Dashboard is a publicly available website. To improve the security of the site, all new and current Dashboard users are required to use two-factor authentication when signing in.

For new Dashboard Users

Per current functionality, an invitation email is sent to new FMH Dashboard users with a link they can click to begin the account creation process. The user can then create a user name and password.

Next, users are asked to set up two-factor authentication for their account. Users can select one of several methods to receive a verification code that they must enter to sign in to their account.

Setup two-factor authentication for your account.

Adding this extra layer of security is required to make sure only you can access your account. You'll need to enter a verification code when logging in to your account. This code can be sent to you via email, text message, or through a smartphone app like Google or Microsoft Authenticator apps. (A new code will be sent every time you log in.)

How would you like to receive your verification code?

- Email
- Text Message
- App

Continue

- If users select **Email**, the user's email address is shown.
- If users select **Text Message**, they will need to enter a valid mobile phone number.
- If users select **App**, a QR code is displayed. Users must use their third party authentication app to scan the QR code.

Users then click **Continue** and a verification code is sent to users using the selected method. Users then retrieve the code from their email address, mobile phone, or authentication app and

enter it in the **Verification Code** field. If an incorrect verification code is entered, an error message is displayed. For email and text message methods, users can click **Resend verification code** as many times as needed to get a new code.

After creating the account and setting up two-factor authentication successfully, new users are asked (per current functionality) to enter the Invite Code they should have received from their provider. When the invite code is accepted, users are taken to the FollowMyHealth Dashboard.

When users sign in again to the FMH Dashboard, they must use the two-factor authentication method to sign in, each time with a new verification code.

For existing Dashboard Users

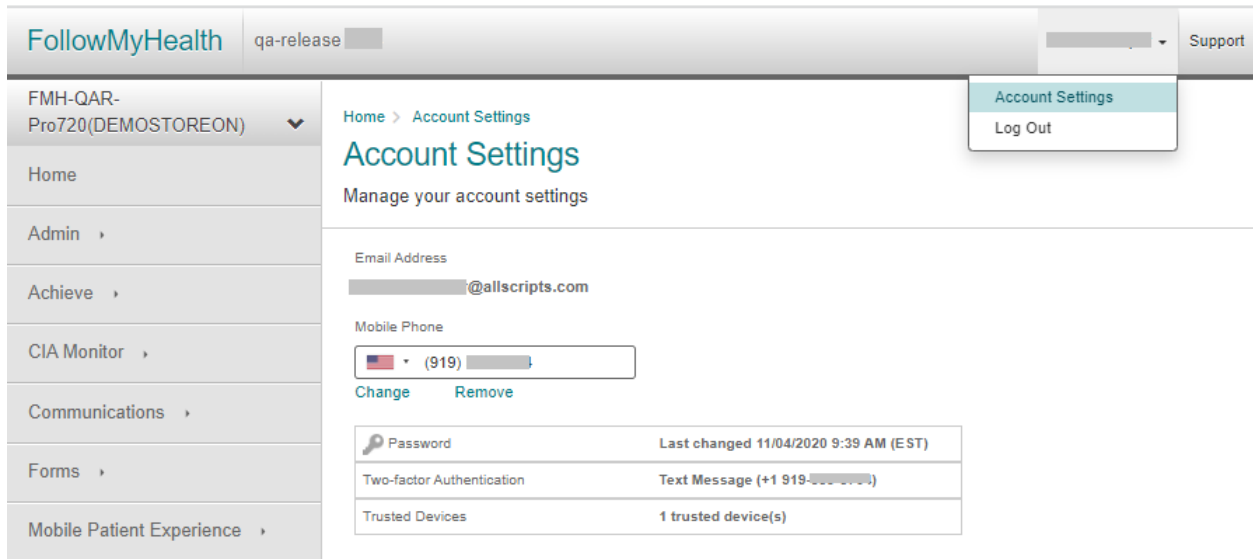
When Dashboard users who have not already configured two-factor authentication sign in, they are asked to set up two-factor authentication for their account. Users must select one of the methods (same as above) before they can continue, following the same workflow to obtain and enter a unique verification code each time they sign in.

Changing the two-factor authentication method

FMH Dashboard users with a FMH Secure Login account who already have a two-factor authentication method configured can access user settings to manage their two-factor authentication settings.

When FMH Dashboard users sign in, the banner across the top includes a link with the user's name in the top right corner. Users can click their name link to display the **Log Out** option, along with the **Account Settings** option. Users can click **Account Settings** to display the following configuration options:

- The user's email address (read-only, cannot be changed)
- The user's mobile phone number (with country code flag icon) and **Change** and **Remove** action links
If no mobile number is available, an **Add a mobile number** link is displayed.
- The date and time the user last changed their password.
- The type of two-factor authentication, if any, configured for their account.
- The number of Trusted Devices, if any, configured for their account.



FollowMyHealth | qa-release | Support

FMH-QAR-Pro720(DEMOSTOREON) | Home > Account Settings

Account Settings

Manage your account settings

Email Address: [redacted]@allscripts.com

Mobile Phone: (919) [redacted]

Change Remove

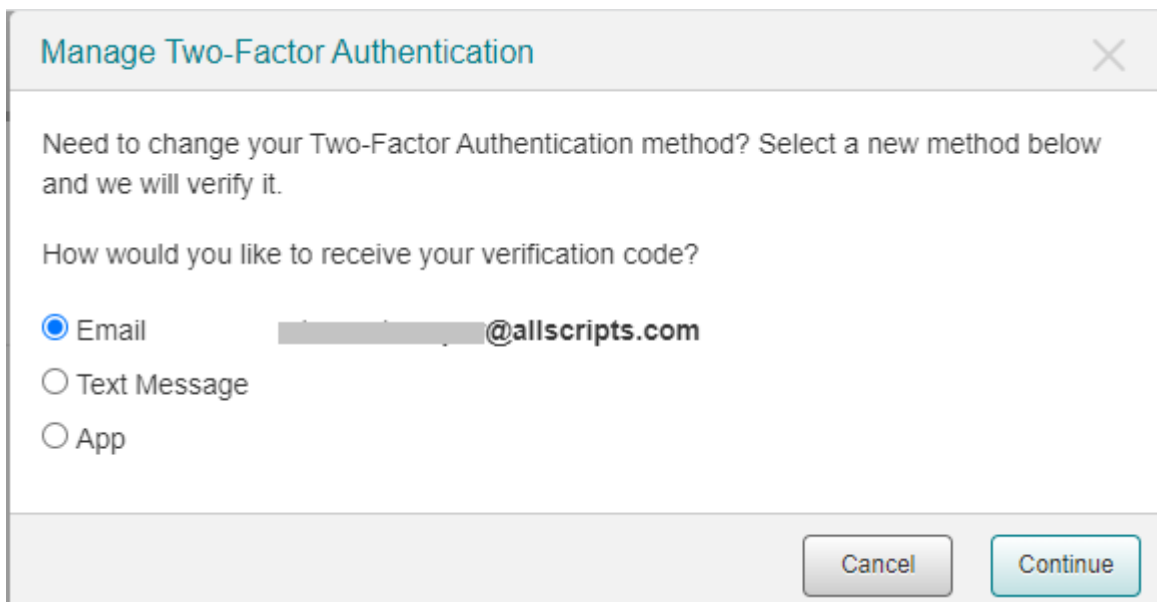
Password	Last changed 11/04/2020 9:39 AM (EST)
Two-factor Authentication	Text Message (+1 919-[redacted])
Trusted Devices	1 trusted device(s)

Users can click in the **Two-factor Authentication** row on the **Account Settings** screen to open the **Manage Two-Factor Authentication** panel.

If a method is already configured for the account, it is shown as selected, with the current destination for receiving verification codes (such as an email address, a mobile phone number, or an app).

Users can click a different option to change the authentication method:

- If **Email** is selected, when the user clicks **Continue** a verification code is sent to the configured email address. The user must retrieve the verification code from their email and enter it in the field provided to confirm the authentication method.



Manage Two-Factor Authentication

Need to change your Two-Factor Authentication method? Select a new method below and we will verify it.

How would you like to receive your verification code?

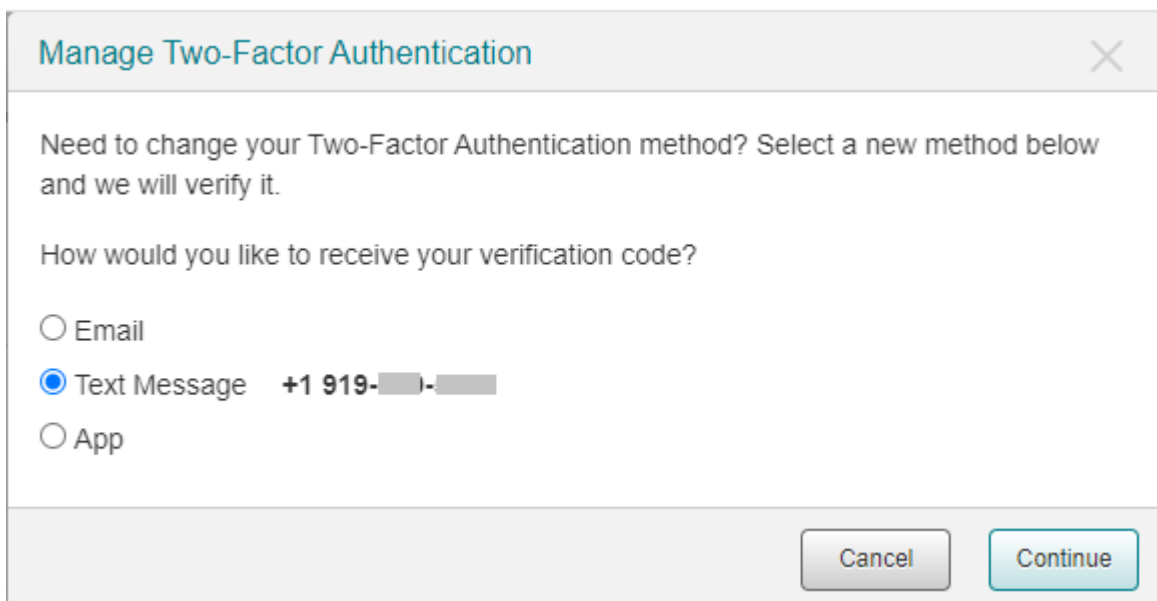
Email [redacted]@allscripts.com

Text Message

App

Cancel Continue

- If **Text Message** is selected, when the user clicks **Continue** a verification code is sent to the configured mobile phone number. The user must retrieve the verification code from their mobile phone text message and enter it in the field provided to confirm the authentication method.



Manage Two-Factor Authentication ✕

Need to change your Two-Factor Authentication method? Select a new method below and we will verify it.

How would you like to receive your verification code?

Email

Text Message +1 919-██-██

App

- If **App** is selected, a QR code is displayed with instructions to scan the QR code with the user's authenticator app. When the user scans the QR code and clicks **Continue**, the user can then go to the authenticator app for a verification code, and enter it in the field provided to confirm the authentication method.

Manage Two-Factor Authentication ✕

Need to change your Two-Factor Authentication method? Select a new method below and we will verify it.


How would you like to receive your verification code?

Email

Text Message

App

Scan the QR code below with your authenticator app. Once scanned, click 'continue' to verify your app is synced with this account. If you plan to use an authenticator app on multiple devices, scan this code on each device before continuing.



Users can click **Resend Verification Code** to resend the code as many times as needed.

When the two-factor authentication method is confirmed, the user is returned to the **Account Settings** screen to view the new authentication method displayed.

Additional notes for FollowMyHealth Dashboard App users

For FollowMyHealth Dashboard users who use the Mobile Android or iOS Dashboard apps, when users download and install the latest FMH Dashboard app, any previous biometric login or passcode login (Touch ID, Face ID, and PIN codes) that users had previously set up are revoked automatically. Users must sign in to the Dashboard App with their FollowMyHealth user ID and password, and then must set up for two-factor authentication. When this is verified, users are then launched into the Dashboard App and can reconfigure their biometric or passcode methods.

When setting up for two-factor authentication using an authenticator app, users can either scan the QR code or click **Copy Key** and enter it into their authentication app. If the app asks for an

account name, users can use FollowMyHealth. If users plan to use the authenticator app on multiple devices, they must scan or enter the key on each device before saving.

How would you like to receive your verification code?

- Email
- Text Message
- App

Scan or copy the key below and enter it in the authenticator app you want to use. If your app asks for an account name, you can use \"FollowMyHealth\". If you plan to use an authenticator app on multiple devices, scan or enter this key on each device before saving.



[Copy Key](#)

Resetting two-factor authentication

FMH Dashboard administrators can be granted permission to force a reset of the two-factor authentication method configured by users in the event the user can no longer use their selected method.

For example, a Dashboard user with verification by text message loses their mobile phone and has a new number, or the user selected to use an authenticator app on their smart phone but loses the phone so the method must be reset.

New permission

FMH Dashboard administrators with the **All Admin** role can be granted the **Reset Two-Factor Authentication** User permission.

Home > Admin > User Roles > All Admin

All Admin

Add New Users to Role

Permissions	Users
delete their own account. Any user role with this permission automatically inherits View Users and View User Roles security permissions.	
<p>Edit Users</p> <p>End-Users with this security permission assigned can select Users from Dashboard Side Menu to edit User Active/Inactive Status, Name, Email Address, and User Role assignments and can also assign users to roles if accessing from Admin > User Roles or Admin > Users. Any user role with this permission automatically inherits View Users and View User Roles permissions.</p>	<input checked="" type="checkbox"/>
<p>Initiate FollowMyHealth Dashboard Login Recovery</p> <p>End users with this security permission will be able to send username and password reset links to the email address on file for the dashboard user. Any user role with this permission automatically inherits the View Users security permission.</p>	<input checked="" type="checkbox"/>
<p>Reset Two-Factor Authentication</p> <p>End users with this security permission can initiate a reset of Two-Factor Authentication for the selected user(s) from the Dashboard Side Menu > Admin > Users. This will force the user(s) to reset their Two-Factor Authentication upon their next log in to the Dashboard. Any user role with this permission automatically inherits the View Users security permission.</p>	<input checked="" type="checkbox"/>
<p>View Users</p> <p>End-Users with this security permission assigned can select Users from Dashboard Side Menu and/or User Roles > [specified user role] > Users and view all active and inactive users that exist within the organization. Any user role with this permission automatically inherits View User Roles security permission.</p>	<input checked="" type="checkbox"/>

Users with this permission can select the **Action > Reset Two-Factor Authentication** option for another Dashboard User and remove the configured authentication method. The next time the user signs in to the Dashboard, they must once again set up their two-factor authentication method to access the Dashboard.

Additional columns added to Admin > Users table

The **Admin > Users** table includes two columns, **Two-Factor Authentication** and **Mobile Phone**. These columns display the authentication method, if any (Email, Text Message, or App), selected by the user and their mobile phone number, if available.

Users Create New User

Create and edit the settings of your users.

test

Last ▲	First ▲	Status	Email	Two-Factor Authentication	Mobile Phone
Admin	Heather	Invited	adminstaff@gmail.com		
Dash	Riprock	Active	rirock@me.com	Text Message	919-552-4411
Duck	Donald	Invited	ddone@me.com		
Nurse	Nancy	Inactive	nancynurse@me.com	Email	919-552-4411
PATEST	Roberta	Active	PAone@gooddr.com	No FMHSL	704-302-1100
PATEST	SAMMY	Active	SAMMYPA@gooddr.com	App	

If there is no FMH Secure Login account for the user (that is, the user signs in by an alternative method, such as Google or another app), the **Two-Factor Authentication** columns displays **No FMH SL**.

Reset action on Admin > Users screen

When Dashboard users with the **Reset Two-Factor Authentication** permission display the list of users (**Admin > Users**) and move the cursor over a user in the list, the **Action** drop-down at the far right displays the option, **Reset Two-Factor Authentication**.

Users Create New User

Create and edit the settings of your users.

test

Last ▲	First ▲	Status	Email	Two-Factor Authentication	Mobile Phone	
Admin	Heather	Invited	adminstaff@gmail.com			
Dash	Riprock	Active	rirock@me.com	Text Message	919-552-4411	
Duck	Donald	Invited	ddone@me.com			
Nurse	Nancy	Inactive	nancynurse@me.com	Email	919-552-4411	
PATEST	Roberta	Active	PAone@gooddr.com	No FMHSL	704-302-1100	
PATEST	SAMMY	Active	SAMMYPA@gooddr.com	App		
Rubble	Barner	Active	prehisroticdude@stonetab...	Email		
Teststaff	Tammy	Active	tammyteststaff@allscripts.com	Text Message	919-444-5555	Actions ▼

- Delete User
- Edit/View Details
- Recover FollowMyHealth Dashboard Login
- Reset Two-Factor Authentication

When this option is clicked, the Administrator is asked to confirm the request. When confirmed, any two-factor authentication method that is displayed in the **Two-Factor Authentication** column of the table for the selected user is removed. This action is also logged with an audit.

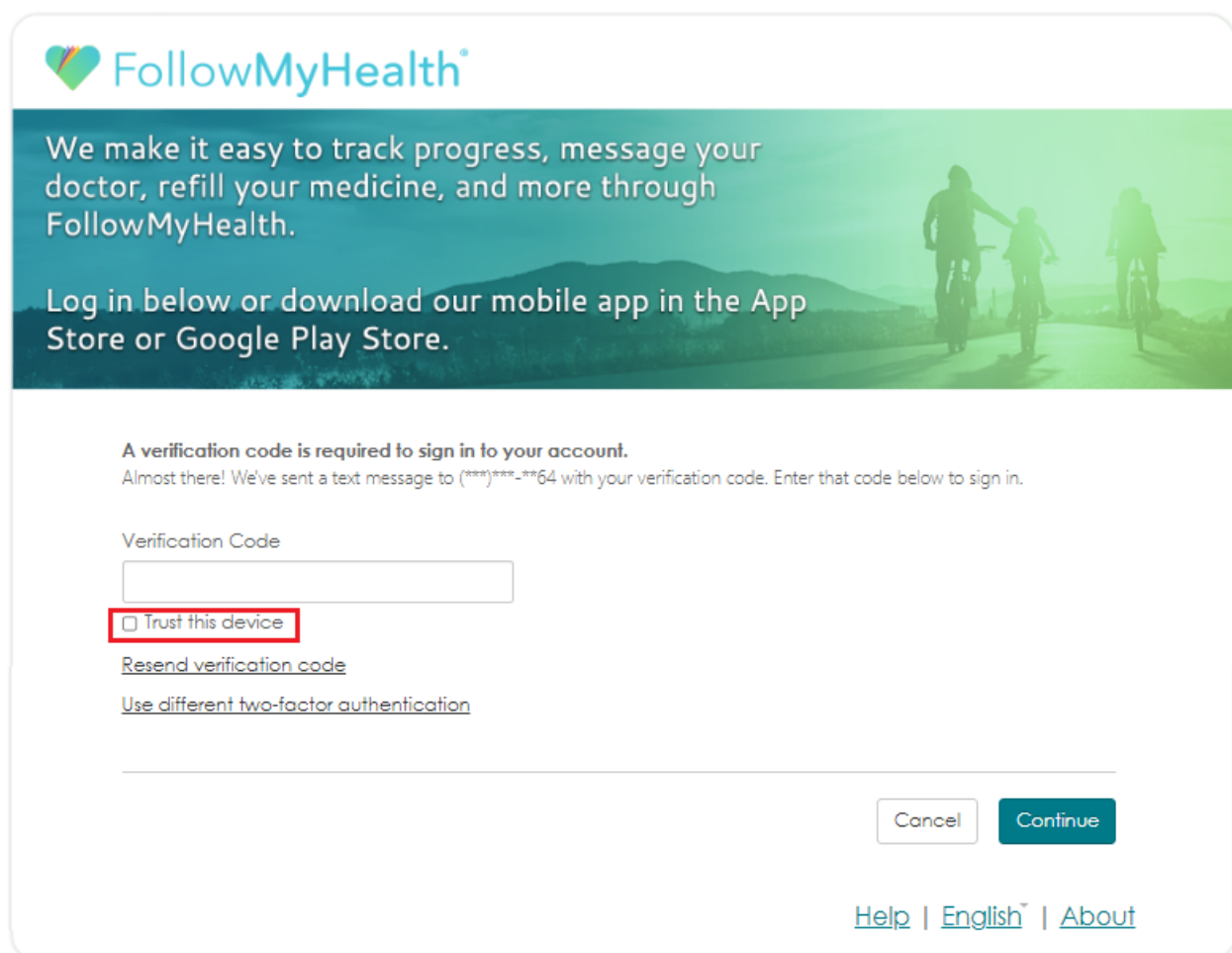
Audit log


When the two-factor authentication method of a Dashboard user is reset, the **Dashboard User Two-Factor Authentication Reset** audit is logged.

Managing trusted devices

When Dashboard users sign in to the FMH Dashboard, instead of entering a two-factor authentication verification code on every sign-in, they can designate their device as a “trusted device”, so they need only sign in with their username and password, and avoid two-factor authentication the next time they sign in on that device.

When Dashboard users sign in on a non-trusted device, they can now select a **Trust this device** checkbox on the 2-factor authentication screen to remember this as a trusted device.



 FollowMyHealth

We make it easy to track progress, message your doctor, refill your medicine, and more through FollowMyHealth.

Log in below or download our mobile app in the App Store or Google Play Store.

A verification code is required to sign in to your account.
Almost there! We've sent a text message to (***)*-***64 with your verification code. Enter that code below to sign in.

Verification Code

Trust this device

[Resend verification code](#)

[Use different two-factor authentication](#)

Cancel Continue

[Help](#) | [English](#) | [About](#)

Trusted Devices will remain saved for up to 14 days. Each time users sign in on a Trusted Device, the expiration period resets to 14 days once again. When a user signs in from a trusted device the Two-Factor Authentication screen is skipped and they are taken directly into their FMH Dashboard account after successfully entering their username and password.

When Dashboard users have at least one trusted device, on their **Account Settings** page a new **Trusted Devices** section is displayed, showing a count of the number of saved trusted devices for the user.

[Home](#) > [Account Settings](#)


Account Settings

Manage your account settings


Email Address

FirstName.LastName@veradigm.com

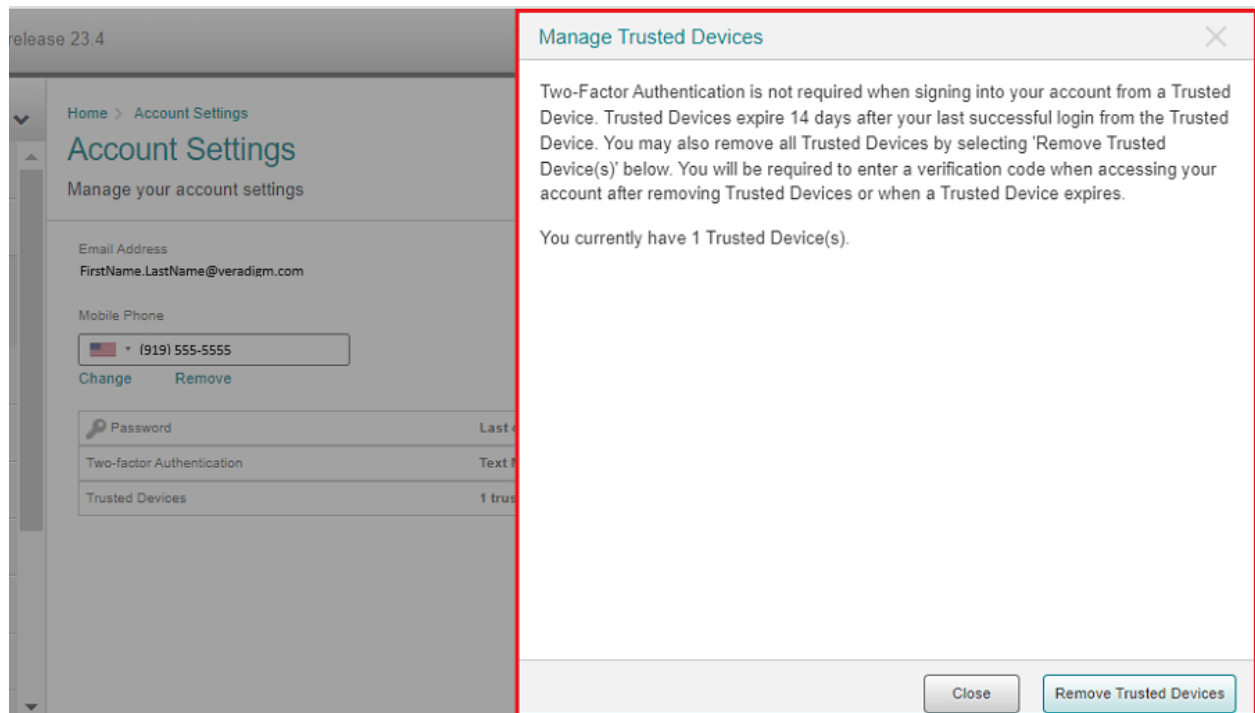
Mobile Phone

 (919) 555-5555

[Change](#) [Remove](#)

 Password	Last changed 11/04/2020 9:39 AM (EST)
Two-factor Authentication	Text Message (+1 (919) 555-5555)
Trusted Devices	1 trusted device(s)

Users can click in this section to open the **Manage Trusted Devices** drawer, from which users can remove all of their trusted devices if needed.



Note: Certain actions within the Dashboard result in the removal of all trusted devices:

- When Dashboard users change or remove their mobile phone number.
- When Dashboard users change their Two-Factor Authentication method.
- When Dashboard users reset their Two-Factor Authentication under **Admin > Users**.



FollowMyHealth Dashboard Users

Personal Health Record Users

Managing sign-in preferences

As part of managing your sign-in preferences, after you create a username and password, you can add another layer of authentication to secure your account.

Two-factor authentication provides a new verification code each time you sign in with your username and password.

The verification code is sent to you through one of the following methods:

- Email
- Text message
- An authenticator app, such as Google or Authenticator

After you sign in to your account, the two-factor authentication sign-in page opens and the verification code is sent to you through your chosen method. Enter the verification code on the two-factor authentication sign-in page to complete the sign-in process.

Add two-factor authentication to your account

Use two-factor authentication with your account to add an extra layer of security to your account. Two-factor authentication is available under **My Account > Preferences > Sign In Preferences**, as long as you have a username and password. If your email address or mobile phone number is not verified, a reminder displays in the **Action Center**.

1. Sign in to the .
2. From the static toolbar, click **My Account > Preferences**.
3. Click **Sign In Preferences**.
4. In **Two-Factor Authentication**, highlight the row to edit.
5. Select one of the following methods to add two-factor authentication to your account.
 - Select **Email**.
Select this option to receive a verification code to the notification email address that is configured in **Communication Preferences**.
 - a. Confirm your email address.

|| **Note:** You need only to verify your email when setting the two-factor preference, if it has not already been verified.

- b. Click **Continue**.
- c. Enter the verification code.
- d. Click **Verify Email**.
- e. After you verify your email address, click **Save**.

|| **Note:** If your connected organization enabled demographics updates, you can choose to send your changes to the organization.

- Select **Text Message**.
Select this option to receive a verification code through a text message on your mobile phone.

- a. Enter your phone number in **Mobile Phone**.
- b. Click **Continue**.
- c. Enter the verification code.
- d. Click **Verify Mobile Phone**.
- e. After you have verified your mobile phone number, click **Save**.

|| **Note:** If your connected organization enabled demographics updates, you can choose to send your changes to the organization.

- Select **App**.
Select this option to receive a verification code through an authenticator application on your smart phone.
 - a. With the authentication app of your choice, scan the QR code provided on the page, then click **Continue**.
 - b. Enter the verification code displayed in the authentication app.
 - c. Click **Verify & Save**.
The **Two-Factor Authentication** field displays your chosen method.
If you change your two-factor authentication method, it is logged in your **Activity History Log**.
 - If switched to **Email**, **Two-Factor Authentication set to Email**, is logged displaying the email address at the time of the change.
 - If switched to **Text Message**, **Two-Factor Authentication set to Text Message**, is logged displaying the phone number at the time of the change.
 - If switched to **App**, **Two-Factor Authentication set to App**.

- If switched to **None**, **Two-Factor Authentication Disabled** is logged with no details.

Note: The user must navigate back to the **Preferences** page to see these updates in **Activity History**. If you updated your email or mobile phone number, then **Email Verified** or **Mobile Phone Added** displays in the **Activity History Log**.


Change two-factor authentication to your account

If you no longer want to use your current email address or mobile phone number for the two-factor authentication, perform the following task to change the two-factor authentication to your account.

Before you begin

Changing your email or phone number within the two-factor authentication preferences changes it globally on your account, not only for two-factor authentication.

1. Sign in to the .
2. From the static toolbar, click **My Account > Preferences**.
3. Click **Sign In Preferences**.
4. In **Two-Factor Authentication**, highlight the row to edit.
5. Select one of the following methods to change the two-factor authentication to your account.
 - Select **Email**.
Select this option to send the security code to the notification email address that is configured in **Communication Preferences**.
 - a. Click **Change**.
 - b. Enter the email address to use in **New Email**.
 - c. Click **Continue**.
 - d. Enter the verification code.
 - e. Click **Verify Email**.


Note: If you click  from within the window where you enter the **Verification Code**, a warning message displays. Either click **Cancel** to confirm you want to cancel changing your email address or click **No, Go Back** to continue changing your email address.

- f. Click **Save** or click **Cancel**.

Note: If your connected organization enabled demographics updates, you can choose to send your changes to the organization.

The new email address displays next to **Two-factor Authentication** on the **Sign In Preferences** page.

- Select **Text Message**.
Select this option to send the security code through a text message on your mobile phone when you change your mobile phone number.
 - a. Click **Change**.
 - b. Enter your phone number in **Mobile Phone**.
 - c. Click **Continue**.
 - d. Verify the information on the page.
 - e. Click **Continue**.
 - f. Enter the verification code.
 - g. Click **Verify Mobile Phone**.

Note: If you click  from within the window where you enter the **Verification Code**, a warning message displays. Either click **Cancel** to confirm you want to cancel changing your mobile phone number or click **No, Go Back** to continue changing your mobile phone number.

- h. Click **Save** or **Cancel**.

Note: If your connected organization enabled demographics updates, you can choose to send your changes to the organization.

The new mobile phone number displays next to **Two-factor Authentication** on the **Sign In Preferences** page.

The **Two-Factor Authentication** field displays your chosen method.

If you change your two-factor authentication method, it is logged in your **Activity History**.

Note: The user must navigate to the **Preferences** page to see these updates in **Activity History**. If you updated your email or mobile phone number, then **Email Changed** or **Mobile Phone Changed** displays in the **Activity History Log**.

Turn off two-factor authentication

Turn off two-factor authentication in the if you no longer want to use it.

1. Sign in to the .
2. Click **My Account > Preferences**.
3. Click **Sign In Preferences**.
4. In **Two-Factor Authentication**, highlight the row to edit.
5. Select **None** from the list.
6. Click **Save**.

Signing in with two-factor authentication

If you have two-factor authentication enabled for your account, a verification code is sent to you using your preferred method. Enter the verification code to complete the sign-in process.

After your username and password are accepted, you are redirected to an additional sign-in page to enter your verification code. This code is sent to you either by email, text message, or a third-party authenticator application, depending on how you configured two-factor authentication in your account.

You are limited to three attempts to enter a valid verification code. After three failed attempts, an error message is displayed and your account is locked for five minutes. An email is sent to your account informing you of unusual activity. If you switch authentication methods before your account is locked, you receive an additional three attempts to enter your verification code. Switching methods does not reset the number of attempts for your original method.

You can request a new verification code to be sent by email or text message if you did not receive or could not find the first code that was sent. This option is not available if you use the third-party authenticator application method. You are limited to three resend requests. At the fourth resend request, an error message is displayed and your account is locked for five minutes. An email is sent to your account informing you of unusual activity.

If your account becomes locked due to too many failed sign-in attempts, a message informs you why your account is locked the next time that you attempt to sign in during the lockout period. You can still access your account by using the password reset or username recovery workflows.

You can regain access to your account if you no longer have access to your current two-factor authentication method without having to contact Support (for example, if you lost access to your email or phone).

- If your current two-factor authentication method is by email, you can receive the code by text if you have a verified mobile phone number on your account.

- If your current two-factor authentication method is by text, you can receive the code by the email address on your account.
- If your current two-factor authentication method is by a third-party authenticator application, you can receive the code by the email on your account or by text if you have a verified mobile phone number on your account.

Index

D

Dashboard account settings [15](#)
manage trusted devices [15](#)

F

FollowMyHealth [19, 21, 23](#)
two-factor authentication [19, 21, 23](#)

M

manage trusted devices [15](#)

S

security [19, 21, 23](#)
two-factor authentication [19, 21, 23](#)

T

two-factor authentication [19, 21, 23](#)
adding [19](#)
changing [21](#)
turning off [23](#)



Index