FollowMyHealth®

FollowMyHealth Support for Multi-Factor Authentication
Proprietary Notice
© 2022 Allscripts Healthcare, 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 Allscripts Healthcare, LLC and/or its affiliates, are intended for use by customers and employees of Allscripts Healthcare, LLC and/or its affiliates and others authorized in writing by Allscripts Healthcare, 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 Allscripts Healthcare, LLC and/or its affiliates. For authorization from Allscripts Healthcare, LLC to copy this information, please call Allscripts Global Product Support Services 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 Allscripts Healthcare, LLC and/or its affiliates. Manufacturer is Allscripts Healthcare, 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 Allscripts Healthcare, 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 Allscripts Healthcare, 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 Allscripts Healthcare, 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 Allscripts Software, LLC and/or its affiliates.

All trademarks, service marks, trade names, trade dress, product names, and logos are property of their respective owners. Any rights not expressly granted herein are 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.

Allscripts Patient Administration Solution (PAS) contains barcode components licensed from IDAutomation.com, Inc. These products may only be used as part of and in connection with the Allscripts Patient Administration Solution software.

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
  Two-factor authentication required for Dashboard users.................................................................7
  Reset two-factor authentication method.........................................................................................9

Personal Health Record Users............................................................................................................13
  Two-factor authentication..............................................................................................................13
Overview

To support the FollowMyHealth Quarterly Attestation for 2015 CURES, the following information summarizes the support for Multi-Factor Authentication in both the FollowMyHealth Dashboard and in the FollowMyHealth Personal Health Record.
FollowMyHealth Dashboard Users

Two-factor authentication required for Dashboard users

The FollowMyHealth Dashboard is a publicly available website. To improve the security of the site, all new and current Dashboard users are now 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

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.

**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.
FollowMyHealth Dashboard users are now required to use two-factor authentication to sign in to the Dashboard. Administrators can now be granted a new 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 now be granted the **Reset Two-Factor Authentication** User permission.
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.

**New columns added to Admin > Users table**
The **Admin > Users** table is enhanced to include two new 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.
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**.

**New 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 a new option, **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 a new audit.

**New Audit log**
When the two-factor authentication method of a Dashboard user is reset, the **Dashboard User Two-Factor Authentication Reset** audit is logged.
Personal Health Record Users

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. For more information about configuring two-factor authentication, see the related concept, “Two-factor authentication”.

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.