



## Carelon multi-factor authentication (MFA) migration FAQs for MBM specialty and post-acute providers / external portal users

Beginning late Q3 this year, Carelon Medical Benefits Management (MBM) will begin to roll out multi-factor authentication (MFA) for its [specialty benefits](#) and [post-acute](#) provider portals. A pilot group, consisting of MBM specialty provider portal users will go first late August to be followed by a rollout schedule for our existing MBM in waves until all users have been migrated.

Please note that our existing post-acute portal users will be migrated in one wave late Q3. New portal users who sign up with us starting in late Q3 will automatically experience the new multi-factor authentication login process.

### 1) What is multi-factor authentication (MFA)?

Multi-factor authentication (MFA) is a multi-step login process that requires system users to enter their username and password followed by additional information such as a code sent to their email or in the future, a code sent via a downloadable phone application. In some cases, the additional authentication step may involve answering a secret question that's been set up ahead of logging in. Another name that is commonly used for this type of authentication is two factor authentication or 2FA.

### 2) Why is MFA important?

Companies commonly use MFA authentication today to protect their own systems, but also to protect those using their systems. Requiring MFA helps protect all against security issues such as compromised login information and phishing attempts. A phishing attempt is an email that tries to obtain confidential information like credit card numbers, usernames or passwords.

### 3) What if I don't migrate within the 30-day grace period?

Once the 30 days has passed, you will be prompted to migrate to MFA. You will not be able to login until you migrate.

### 4) Can I use my personal email address as a username?

It is preferred that you use an email address that indicates your organization, but you can use any email address as a username.

### 5) What if I entered my new username/email address incorrectly?

You can restart the migration process by logging in with your previous username. Your account will not be migrated until you have confirmed the one-time passcode (OTP) sent to your email address.



6) What if I don't receive the email with the one-time passcode (OTP)?

During the migration process, verify that the username/email address shown on the Email Verification page is valid. If it is not valid, restart the migration by logging in with your previous username.

If username/email address is valid, check your spam/junk folder.

You can also select to have the code resent to you by clicking on the "Resend Email" link on the Email Verification page.

7) What if I migrated but accidentally enter my old username the next time I login?

You will not be able to login with your old username.

8) What if I want to change the email address I am using as a username?

This feature will be implemented in an upcoming release.

9) What if I forgot my password?

Click on the "Can't access your account?" link on the User Confirmation page.

10) What if I don't like the new password I created?

You will be able to reset your password after 1 hour. You are not able to reset your password again within an hour for security reasons.

11) What options do I have for MFA?

Currently only one time passcode (OTP) via email, but there will be additional options in the future including a downloadable phone application.

12) How can I stay informed of the rollout schedule and additional information?

Check our Provider Connection [Portal updates blog page](#) and our [post-acute provider Welcome page](#) regularly for the latest information and important dates tied to our MFA rollout. FAQs will be shared in conjunction with the go live date. Aqs will be shared in conjunction with the go live date.