HealthEquity®
15 W. Scenic Pointe Dr. Suite 100
Draper, UT 84020
P: 855.437.4727
F: 801.727.1005
www.HealthEquity.com
info@healthequity.com

Multi-factor authentication

Frequently asked questions

EXTERNAL-FACING

1. **What is multi-factor authentication (MFA)?**
   MFA is an online security process that governs a member's access to the HealthEquity member portal. MFA requires multiple pieces of information during the login process to verify the identity of the person logging-in and consists of the following three distinct, but separate processes or states:
   a. E-mail Verification (Login – Security Verification)
   b. Account Lock-out
   c. Identity Proofing (Identity Verification)
2. **Why is the login experience changing?**
   HealthEquity is continually improving our security features to protect our members. Additional security enhancements, including updates to MFA, may be made in the future.
3. **Who is required to use MFA?**
   ALL members who login to the HealthEquity member portal will be required to complete MFA each time they use a new computer or device to access the portal.
4. **With MFA, is an email address required for portal access?**
   Yes. If a member does not have an email address on file the member will be required to proceed through the identity verification process first. Upon successfully verifying their identity they will then be prompted to enter an e-mail address that will need to be verified.
5. **What is the MFA process?**
   When members enter their username and password into the HealthEquity member portal login screen, the member may pass through one or all of the following:
   - **E-mail Verification (Login – Security Verification)**

     This is the process that requires members to input, have access to or confirm the following:
     - Input the correct username and password
     - Have access to an external e-mail account where a confirmation code can be retrieved
     - Input or confirm a primary phone number for password recovery purposes

     Upon successfully entering the correct username and corresponding password, retrieving and entering the correct confirmation code received from the external e-mail account the member has access to and entering or confirming a primary phone number, the member is granted full access to their account.

- **Account Lockout**

  This is a state that the member will be put in when the member fails multiple times to provide a correct username and password (5 attempts allowed), fails e-mail verification or cannot pass the Lexis Nexis identity proofing process. Members in a lock-out state will not be able to login to their account for three hours, unless manually unlocked by a HealthEquity representative. The member can contact member services to request assistance when this occurs or wait until the lock-out period has expired.

  NOTE: For security purposes, the member is NOT informed of the duration of the lock-out period through the user-interface.

- **Identity Proofing (Identify Verification)**

  This is the process the member proceeds through in the event that they select "I don't recognize this e-mail address" or the system doesn't have the member's e-mail address on file. This process uses the following third-party tools to verify the member's identity which will then allow them to enter or update specific contact information:

  - Lexis Nexis Text / Voice (ID-OTP): This tool verifies a phone number entered by the member so that a confirmation code can be sent via text or voice depending on the member's preference. Successful verification of the entered phone number allows the member to enter or update select contact information (E-mail address (required), primary phone number (required) and phone number 2 (optional)). Upon successfully entering or updating this information the system directs the member to the e-mail verification process outlined above.

    Failure to receive confirmation from Lexis Nexis that the phone number entered is accurate or failure to enter the accurate confirmation code without exceeding the allowable attempts will result in the member's account being locked-out.

  - Lexis Nexis Knowledge Base Authentication (KBA): This tool presents the user with 3-5 questions about their background (e.g. places they have lived, members of their family, property that they have owned) pulled from the Lexis Nexis knowledge base to verify the identity of the member. It is presented to the member in the following ways:

    - Upon selection of the "Answer security questions" hyperlink displayed to the member if the member hasn't reached the allowable attempts for entering the confirmation code
    - The Member doesn't have an e-mail address on file AND have failed ID-OTP within the last three hours

    Upon successfully answering the questions presented, the member is allowed to update their contact information (E-mail address (required), primary phone number (required) and phone number 2 (optional)) and will proceed to direct the member to the e-mail verification process

15 W. Scenic Pointe Dr. Suite 100
Draper, UT 84020
P: 855.437.4727
F: 801.727.1005
www.HealthEquity.com
info@healthequity.com

outlined above. If the questions are answered incorrectly the member is locked-out of the account.

NOTE: For security purposes, the member is NOT informed of the duration of the lock-out period through the user-interface.

6. **How often will MFA be required?**
   Each time a member accesses the portal from a new device, does not select 'Remember this computer' or clears their browser cache after logging in, he/she will be prompted to go through the MFA process. In addition, the login process may continue to evolve as HealthEquity adds new security features. When this happens, members may be required to complete new security steps when they log in after updates are made.

7. **How does MFA help protect members' accounts?**
   MFA provides an additional layer of security beyond login credentials. If an attacker attempts to login to a member's account using stolen login credentials from an unrecognized computer or device, the attacker will be confronted with MFA. If the attacker is unable to provide a second factor of authentication, access to the account is denied.