
# Healthfully

## Multi-Factor Authentication (MFA) Use Cases

*Kristen Hostetter, VP of Development*

## Healthfully, Healthfully Practice Workspace

Healthfully and Healthfully Practice Workspace support multi-factor authentication (MFA) using industry-standards in alignment with the Office of the National Coordinator for Health IT's (ONC) Multi-factor authentication criterion at 45 CFR 170.315(d)(13) for the following workflows:

- User authentication during sign-in

The following MFA options are supported for each of the above workflows:

- **Healthfully second factor authentication with One Time Password (OTP) token:** Healthfully provides a multi-factor authentication solution that does not require third-party software or hardware. Healthfully second factor authentication with Healthfully OTP token leverages on a time-based time-finite token generation algorithm, that ensures that only a single user may have received a single token to perform authentication. The token is being delivered to the user via SMS to his phone number or email, defined in his user account. User may enable or disable OTP MFA for his account in user profile settings after successful authentication.

## Healthfully Mobile

Healthfully mobile applications support multi-factor authentication (MFA) using industry-standards in alignment with the Office of the National Coordinator for Health IT's (ONC) Multi-factor authentication criterion at 45 CFR 170.315(d)(13) for the following workflows:

- User authentication during sign-in

The following MFA options are supported for each of the above workflows:

- **Healthfully second factor authentication with One Time Password (OTP) token:** Healthfully provides a multi-factor authentication solution that does not require third-party software or hardware. Healthfully second factor authentication with Healthfully OTP token leverages on a time-based time-finite token generation algorithm, that ensures that only a single user may have received a single token to perform authentication. The token is being delivered to the user via SMS to his phone number or email, defined in his user account. User may enable or disable OTP MFA for his account in user profile settings after successful authentication.
- **Platform-native biometrics authentication:** Healthfully provides platform-native biometrics authentication (FaceID, TouchID and others vendor-specific technologies) methods during user sign-in process as a layer of second factor authentication. Exact implementations of used methods are provided by the platform vendor and are leveraging on vendor-provided

developer guides for best user experience. User may enable or disable Biometrics MFA for his account in user profile settings after successful authentication.

## Healthfully Administrative Panel

Healthfully Administrative Panel requires multi-factor authentication (MFA) using industry-standards in alignment with the Office of the National Coordinator for Health IT's (ONC) Multi-factor authentication criterion at 45 CFR 170.315(d)(13) for the following workflows:

- Admin user authentication during sign-in

The following MFA options are supported for each of the above workflows:

- **Healthfully Administrative Panel second factor authentication with One Time Password (OTP) token:** Healthfully Administrative Panel provides a multi-factor authentication solution that does not require third-party software or hardware. Healthfully Administrative Panel second factor authentication with Healthfully OTP token leverages on a time-based time-finite token generation algorithm, that ensures that only a single admin user may have received a single token to perform authentication. The token is being delivered to the admin user via SMS to his phone number defined in his user account. The admin user cannot disable MFA as a second factor authentication during sign-in process to administrative panel.