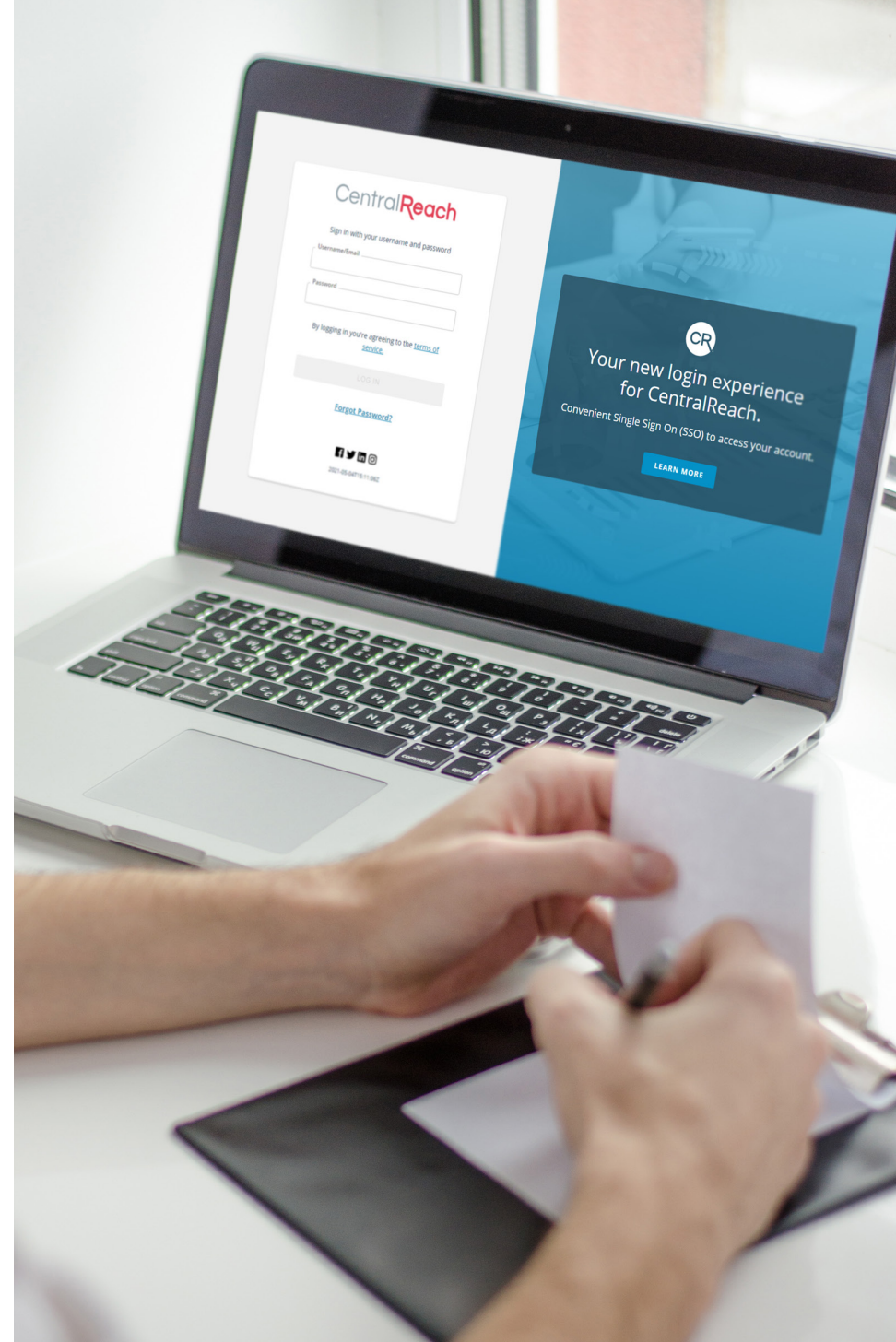
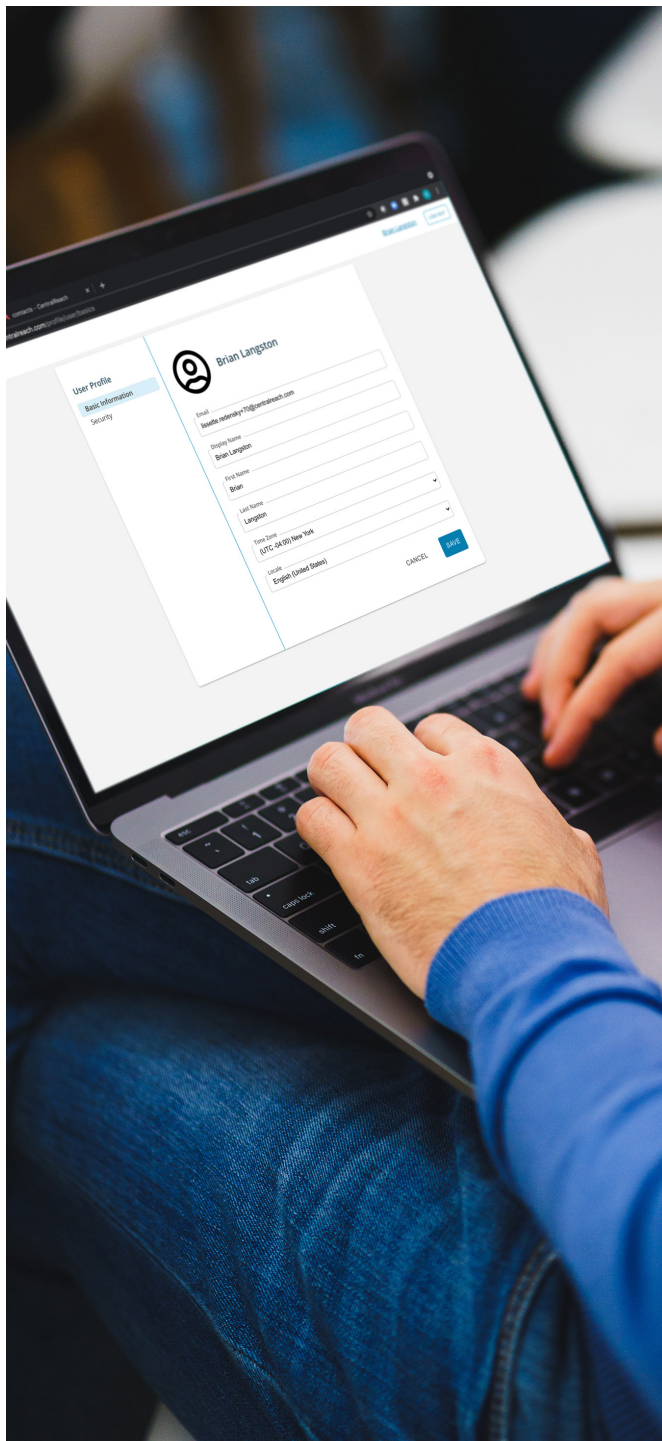




Your new CentralReach login experience.

Gain leading security and control over your CentralReach account, with convenient Single Sign On (SSO) and recommended Multi-Factor Authentication (MFA) for CentralReach.





Your new login experience.

Protect your CentralReach account from common threats like phishing attacks and account takeovers. The new login experience provides improved security and traceability for the Personal Health Information (PHI) and Personally Identifiable Information (PII) in your CentralReach account.

A simple swap from username to email address

When the new login experience arrives, you'll be redirected to a new login screen. There, you'll walk through a short process that will switch you from using a username to using a validated, unique email address.

Before, users logged into CentralReach with a username.

Now, users will log into CentralReach with a unique email address. This protects against phishing, as the unique email address is validated to confirm each user is who they say they are. This also paves the way for Single Sign On (SSO), so users can log into multiple CentralReach products using the same credentials

A new page to easily manage your login credentials

Once logged into CentralReach, you'll see two small updates. Now, your menu drop-down will include a new link to "Single Sign On Settings" where you can manage your name, email, password, MFA options, and more.

Also, you'll see the "Single Sign On Settings" page when clicking Profile > Login & Access.



Optional Multi-Factor Authentication (MFA)

Your organization will decide whether or not to enable Multi-Factor Authentication (MFA): a powerful, familiar way to confirm your identity when accessing sensitive information like online banking details or electronic health information.

If your organization enables MFA, the new login experience will walk you through a short process to set it up. You may choose from three options: 1) an authenticator app, which is the most secure, 2) email authentication, or 3) SMS text message authentication

Before, users logged into CentralReach with a username.

Now, users will log into CentralReach with a unique email address. **Then**, users will confirm their identity with a 6-digit code from one of the following:

1. An authenticator app (*Microsoft Authenticator, Twilio Authy, or Google Authenticator. These are freely downloadable from the iTunes and Googleplay stores.*)
2. A validated email address

MFA keeps your CentralReach information safe.

The small, recommended step of MFA is simply the best way to protect your account from common threats like phishing and account takeovers. It utilizes both a factor you know (your email/password) and a factor you have (your app, email, or phone) to verify your identity and prevent bad actors from accessing your account.

Please remember to follow your organization's policies for MFA, including the preferred MFA options (app, email, or SMS).