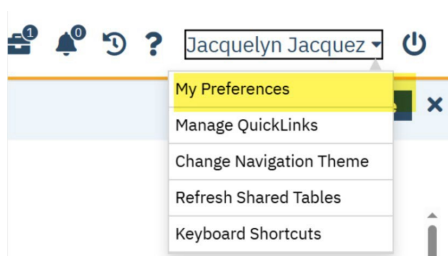# SmartCare Multi-Factor Authentication

To ensure the best possible security of client data, the County will be rolling out multi-factor authentication (MFA) to all contracted users on Tuesday, November 19. This means that after entering user ID and password, users will receive an email with a one-time code that will need to be entered before gaining access into the system. Users will use MFA each time they access SmartCare. The change will not impact users who log in via Akamai with a County email.

Instructions to Update Your Contact Information for Multi-Factor Authentication

Log in to the SmartCare Production Environment using [this link](#).
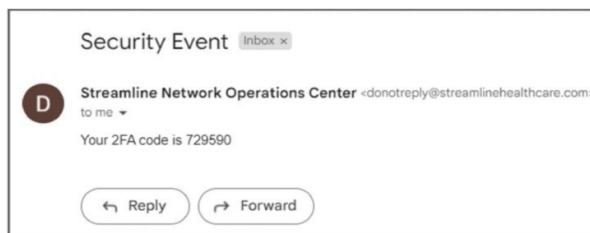
The default is set to receive the 6-digit code to your email for login.

To update or add a mobile phone number and/or email, navigate to "My Preferences."

Then, update or add a phone number and email in the Contact section under "My Preferences"

For questions about MFA in SmartCare's Production environment, contact the CalMHSA help desk.

SmartCare Multi-Factor Authentication

Select the checkbox for "Registered For SMS Notifications" in the Mobile section to enable SMS text MFA. Send a test notification to both options to ensure phone number and email are correct.

*If **both** SMS & email are checked, the notification will default to the SMS phone number given

Instructions for Login After Setting Up MFA

Enter your normal username and password on the first login screen.

If the second authentication method is email, answer the security question and enter the code sent by email.

If the second authentication method is SMS text, enter the code sent by SMS text.

For questions about MFA in SmartCare's Production environment, contact the CalMHSA help desk.