



*We heal and inspire the human spirit.*

**To:** EVV Impacted Providers and Individual Nurse Providers

**From:** IEHP – Provider Relations

**Date:** January 24, 2024

**Subject: Required: Multi-factor Authentication (MFA) – February 21, 2024**

---

---

**Effective February 21, 2024:** Multi-factor Authentication (MFA) will be required to access the CalEVV Portal and Aggregator. Instructions to log in using MFA are listed below.

### **What is MFA?**

MFA, also referred to as two-factor authentication, is a security method that requires users to provide two or more forms of identification before granting access to an account or system.

### **How does MFA work?**

Typically, MFA involves providing a password or Personal Identification Number (PIN) along with an additional factor, such as a fingerprint or security token, which is a unique passcode generated for users to gain access to the system.

### **Why is MFA important?**

MFA is essential for securing online accounts, particularly those containing sensitive information. Passwords can often be compromised, making them unreliable as a sole method of security. MFA adds an extra layer of security protection and makes it more difficult for unauthorized users to access an account even if they have obtained or bypassed the password.

### **MFA and the CalEVV System**

MFA will be enabled for both the CalEVV Portal and Aggregator. MFA will **not** be enabled for the CalEVV Sandata Mobile Connect (SMC) application. Therefore, no action is required for SMC mobile application users.

### **How to Authenticate?**

Authentication can be validated by using one of the following methods to verify identity:

- Email address associated with your CalEVV user profile
- Google Authenticator
- Microsoft Authenticator

### **How Often?**

MFA will be required every 12 hours, regardless of activity, or when a user logs into the CalEVV system from a new device.

### **Selecting MFA Method at Initial Login**

Once MFA has been enabled for CalEVV, users will be prompted to choose one of two MFA methods:

## Email:

1. The email associated with your profile on CalEVV
2. Authenticator application which can be either of the following:
  - a. Microsoft Authenticator
  - b. Google Authenticator

The screenshot shows a web interface titled "TWO-FACTOR AUTHENTICATION". Below the title, it says "Welcome, your state payer program has chosen to require two-factor authentication." and "Please select authentication type:". There are three buttons: "AUTHENTICATOR APP", "EMAIL", and "CANCEL".

## Instructions for MFA Using Email – Choice #1

1. You will receive an email from [noreply@okta.com](mailto:noreply@okta.com).
  - a. Check your spam/junk folder
2. Open the email, scroll down, and locate your one-time verification code
3. Copy/paste the code into CalEVV MFA when prompted
4. Click SUBMIT

The screenshot shows a web interface titled "TWO-FACTOR AUTHENTICATION". It includes a note: "\* indicates required field". The main text says: "An email has been sent to you with a passcode. Once you have received the passcode, enter 6-digit code below:". There is a text input field labeled "PASSCODE \*" with the placeholder text "Enter Passcode". Below the field are "CANCEL" and "SUBMIT" buttons.

## Instructions for MFA Using Authenticator Application – Choice #2

1. Download either the Google Authenticator or Microsoft Authenticator application
2. Open the application
3. Retrieve the passcode from the application
4. Enter the passcode into CalEVV MFA when prompted
5. Click SUBMIT

## Contacts and Resources

For technical assistance, please call Customer Support at 1-855-943-6070 or email [CACustomerCare@sandata.com](mailto:CACustomerCare@sandata.com).

For Alternate EVV assistance, please call Customer Support at 1-855-943-6069 or email [CAAltEVV@sandata.com](mailto:CAAltEVV@sandata.com)

For additional questions, email:

- DHCS: [EVV@dhcs.ca.gov](mailto:EVV@dhcs.ca.gov)
- DDS: [EVV@dds.ca.gov](mailto:EVV@dds.ca.gov)
- CDA: [EVV@aging.ca.gov](mailto:EVV@aging.ca.gov)
- CDPH: [CDPHMCWP@cdph.ca.gov](mailto:CDPHMCWP@cdph.ca.gov)

The screenshot shows a web interface titled "TWO-FACTOR AUTHENTICATION". It includes a note: "\* indicates required field". The main text says: "To enable Google Authenticator, please follow these steps:" followed by a list of instructions: "1. Install Google Authenticator on your phone", "2. Open Google Authenticator app", "3. Tap plus, then tap 'Scan a QR code'", and "4. Your phone will be in 'scanning' mode. When you are in this mode, scan the QR code below:". Below the text is a QR code. Underneath the QR code, it says: "Once you have scanned the QR code, enter 6-digit code below:". There is a text input field labeled "PASSCODE \*" with the placeholder text "Enter Passcode". Below the field are "CANCEL" and "SUBMIT" buttons. A note at the bottom says: "Note: This passcode is used for Google Authenticator activation. After this, you will be prompted to enter additional passcode for verification."