We heal and inspire the human spirit.

To: EVV Impacted Providers and Individual Nurse Providers

From: IEHP – Provider Relations

Date: December 1, 2023

Subject: **Two (2) DHCS EVV Updates Coming In 2024!**

There are **TWO (2) Electronic Visit Verification (EVV) changes coming in 2024.**

Effective January 1, 2024:

What is changing?
CalEVV services will be updated for the following programs:

- Multipurpose Senior Services Program (MSSP) 1915(c) Waivers
- Home Health Care Services (HHCS) - Managed Care Plan (MCP) and Fee-for-Service (FFS)
- Home and Community-Based Alternatives (HCBA)

Providers who use CalEVV for the above programs, please use the following path to access the updated service codes: DHCS.ca.gov > Providers & Partners > Electronic Visit Verification.

Why are these changes being made?
CalEVV has identified new services that will be added and services that will be removed from the EVV system effective January 1, 2024, to remain in compliance with federal and state requirements.

What are the impacts?

- Provider office staff will update their client-payer records prior to service delivery.
- New HCPCS codes for MSSP, HCBA and Home Health Agency (HHA) services will be added.
- Caregivers logging visits for these programs using CalEVV will choose the new services, starting January 1, 2024.
- The existing MSSP Z codes will be removed and replaced with new Healthcare Common Procedure Coding System (HCPCS) codes and units.

Provider Actions

- Review new services and verify if new services impact your agency.
- Providers will need to update the client payer section for **each** impacted member/client in CalEVV with the new services.

Effective February 1, 2024:

What is changing?

The CalEVV team is targeting to implement Multi-factor Authentication (MFA) to its CalEVV Portal, Aggregator, and Business Intelligence (BI) tool.

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 enter to gain access to the system. By requiring multiple factors of authentication, MFA makes it more difficult for unauthorized users to access an account and therefore protecting CalEVV data.

MFA Requirements:

- MFA can be performed via the valid email address associated with your CalEVV user profile or by using either Google Authenticator or Microsoft Authenticator, which are third-party authentication applications.
- MFA reauthentication will be required every 12 hours regardless of activity for CalEVV Portal and CalEVV Aggregator.
- MFA reauthentication will be required every 24 hours for the CalEVV Business Intelligence (BI) Tool.
- Users will be prompted for an MFA token if the user changes browser and/or device.

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.

Questions?

Contacts and Resources

For general information about the CalEVV program, please visit these California Department EVV websites:
DHCS.ca.gov > Providers & Partners > Electronic Visit Verification or
DDS.ca.gov

For technical assistance, contact 1-855-943-6070 or CACustomerCare@sandata.com. For additional questions, email EVV@dhcs.ca.gov or EVV@dds.ca.gov.