



State of California—Health and Human Services Agency  
Department of Health Care Services



DATE: March 6, 2023

Medi-Cal Eligibility Division Information Letter No.: I 23-13

TO: ALL COUNTY CORRECTIONAL FACILITIES/COUNTY JAILS  
ALL COUNTY YOUTH CORRECTIONAL FACILITIES  
ALL CHIEF PROBATION OFFICERS

SUBJECT: Eligibility Verification Systems (EVS) for County Correctional  
Facilities/County Youth Correctional Facilities - Related to  
ACWDL 22-27  
(Reference Assembly Bill 133 and California Penal Code Section  
4011.11)

The purpose of this letter is to inform County Correctional Facilities and County Youth Correctional Facilities about the Department of Health Care Services' (DHCS) Eligibility Verification Systems (EVS). County Correctional Facilities and County Youth Correctional Facilities and/or their designees can use EVS via the internet, third party software or by an automated phone number to verify Medi-Cal enrollment of incarcerated individuals for the mandatory Pre-Release Medi-Cal Application Process. See, [Assembly Bill \(AB\) 133](#) (Chapter 143, Statutes of 2021), "California Advancing and Innovating Medi-Cal (CalAIM) Initiative." For the purposes of this letter, "CCFs" describes County Correctional Facilities and County Youth Correctional Facilities, and "designees or designated entity or entities" refers to Social Service Departments (SSDs), CCFs, Community Based Organizations (CBOs), or other contracted entity designated by the applicable County Board of Supervisors to assist with submitting the Pre-Release Medi-Cal Application.

### Background

Effective January 1, 2023, CalAIM required all counties to implement a Pre-Release Medi-Cal Application Process to ensure all inmates and youth who are released from CCFs receive timely access to Medi-Cal services, if eligible. DHCS issued [All County Welfare Directors Letter \(ACWDL\) 22-27](#) to establish pre-release Medi-Cal application policy for both CCFs and/or their designees and update existing policy for CWDs.

Per California Penal Code section 4011.11(h), the board of supervisors in each county, in consultation with the county sheriff or chief probation officer, shall

March 6, 2023

designate an entity or entities to assist county jail inmates and youth with applying for, or otherwise assisting their enrollment in, a health insurance affordability program consistent with federal requirements. The designated entity or entities must work together to facilitate the enrollment of inmates and youth in health insurance affordability programs on or before their date of release by developing a process to inform SSDs of the incarceration status of their inmates and youth, for SSDs to appropriately suspend and activate (unsuspend) Medi-Cal coverage for beneficiaries.

### **EVS Access**

Internet Eligibility Verification: CCFs and their designated entity will be granted one account for their organization's staff to access and utilize internet eligibility verification services through DHCS' Medi-Cal Provider website. This service provides an easy-to-understand summary of the individual's Medi-Cal enrollment. EVS can provide enrollment verification in batches for up to 99 records at a time, and CCFs and their designated entity may print the results of the individual's file. CCFs/designated entities do not need to pay for access to EVS.

Other EVS Methods: Medi-Cal enrollment can also be verified by third party software or the Automated Eligibility Verification System (AEVS).

### **Obtaining Access to EVS**

To obtain EVS access, CCFs and/or their designated entity should complete the Medi-Cal Point of Service (POS) Network/Internet Agreement form (see, Enclosure #1) and submit the form to DHCS at [CalAIMJusticePreReleaseApps@dhcs.ca.gov](mailto:CalAIMJusticePreReleaseApps@dhcs.ca.gov). Once the paperwork has been processed, EVS account information will be shared with the CCFs or their designated entity's authorized contact.

### **How to Use EVS**

To understand how to navigate and use EVS, please refer to the User Guide for Pre-Release Medi-Cal Application Processes (see, Enclosure #2). This document will provide guidance on how to verify Medi-Cal enrollment for the Pre-Release Medi-Cal Application process.

### **Account Maintenance and PIN Resets**

Please contact [CalAIMJusticePreReleaseApps@dhcs.ca.gov](mailto:CalAIMJusticePreReleaseApps@dhcs.ca.gov) to:

- Report any changes to account information
- Request a reset of the PIN
- Ask any questions regarding this letter

For CalAIM Justice Involved updates and additional information please visit:

<https://www.dhcs.ca.gov/CalAIM/Pages/Justice.aspx>.

March 6, 2023

Original Signed By

Yingjia Huang  
Assistant Deputy Director  
Health Care and Benefits  
Department of Health Care Services

Enclosure

## MEDI-CAL POINT OF SERVICE (POS) NETWORK/INTERNET AGREEMENT

This agreement is required for all providers and non-providers (provider representatives) who intend to use the Medi-Cal POS Network or Medi-Cal website applications at [www.medi-cal.ca.gov](http://www.medi-cal.ca.gov).

### I.

- (a). The following is required only for enrolled Medi-Cal providers: The Department of Health Care Services (DHCS) will permit the use of the California POS Network and Medi-Cal website by the following Medi-Cal provider subject to the terms and conditions of this agreement.

Provider Name: \_\_\_\_\_

Provider Number/NPI: \_\_\_\_\_ N/A

Owner Number: \_\_\_\_\_ N/A (If applicable)

Tax ID Number: \_\_\_\_\_ N/A

- (b). The following is required only if intending to use a device and/or software that is not obtained through Medi-Cal:

Vendor/Developer Company Name: \_\_\_\_\_ N/A

CMC Submitter Number (if applicable): \_\_\_\_\_ N/A

Contact Person: \_\_\_\_\_ N/A

Phone Number: (\_\_\_\_) \_\_\_\_\_ N/A

- (c). The following is required only for non-provider users [provider representatives] of the POS Network/Medi-Cal website: DHCS will permit the use of the Medi-Cal POS Network and/or Medi-Cal website by the authorized provider representative \_\_\_\_\_ (Representative) subject to the terms of this agreement. When applicable, please attach to this agreement a list of all provider numbers/NPIs and corresponding Tax Identification Numbers (TINs) for which the non-provider user is also the authorized representative.
- (d). Provider/Representative is requesting to delete access and usage of the POS Network and/or Medi-Cal website to the following provider representative \_\_\_\_\_ N/A (Representative) subject to the terms of this agreement. When applicable, please attach to this agreement a list of all provider numbers/NPIs and corresponding TINs for deletion.

### II. Provider/Representative agrees to limit the usage of the POS Network and Medi-Cal website to the following Medi-Cal eligibility and claims-related transactions:

- A. Verification of Medi-Cal eligibility
- B. Share of Cost (Spend Down) clearance
- C. Medi-Service reservations
- D. Submission of Pharmacy claims (may only be performed by providers enrolled to submit claims on the *Pharmacy/Medical Supplies Claim Form*)
- E. Submission of ANSI ASC X12N 837 professional claims (may only be performed by providers enrolled to submit claims on the Medi-Cal Medical Services claim form)
- F. Submission of electronic Treatment Authorization Requests (i.e. eTAR and Pharmacy NCPDP)
- G. Submission of other transactions as may be subsequently permitted by DHCS and as documented in one or more of the user manuals in the Publications area of the Medi-Cal website
- H. Browsing of Medi-Cal website

Provider/Representative acknowledges that failure to limit the usage of the POS Network and/or Medi-Cal website to the transactions described above may, at a minimum, result in DHCS revoking the privilege to use the POS Network and/or Medi-Cal website. Provider/Representative acknowledges abuse of transactions available on the Medi-Cal website may result in DHCS revoking provider access to Medi-Cal website.

- III.** The Provider/Representative agrees that the following constitutes the only authorized methods of accessing the POS Network:
- A. Medi-Cal-provided toll-free (800) line or 916-prefix phone line as documented in the *POS Device User Guide*
  - B. Provider- or Representative-provided leased phone lines
- IV.** Any computer accessing the Medi-Cal website is required to abide by all applicable State and Federal laws enacted today or in the future.
- V.** The Provider/Representative agrees to the following security requirements. All computers that access Medi-Cal data must meet the following requirements, in addition to any State and Federal required administrative, technical, physical, and organizational safeguards:
- A. Antivirus software. All workstations, laptops and other systems that access the Medi-Cal website or process and/or store Medi-Cal Protected Health Information (PHI) must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.
  - B. Patch Management. All workstations, laptops and other systems that access the Medi-Cal Web site or process and/or store Medi-Cal PHI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process, which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.
  - C. System Timeout. The systems that access the Medi-Cal website or process and/or store Medi-Cal PHI must provide an automatic timeout, requiring re-authentication of the user session. It is recommended that the automatic timeout be after no more than 20 minutes of inactivity.
  - D. User Name and Password Controls. Systems that access the Medi-Cal website or process and/or store Medi-Cal PHI should be accessed using a unique user name. The user name must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared. Passwords must be: (1) At least eight characters, (2) A non-dictionary word, (3) Not be stored in readable format on the computer, (4) Be changed every 90 days, preferably 60 days, (5) Be changed if revealed or compromised, and (6) Be composed of characters from at least three of the following four groups from the standard keyboard:
    - Upper case letters (A-Z)
    - Lower case letters (a-z)
    - Arabic numerals (0-9)
    - Non-alphanumeric characters (punctuation symbols)
  - E. Workstation/Laptop encryption. All workstations and laptops that access the Medi-Cal website or process and/or store Medi-Cal PHI are recommended to be encrypted using a FIPS 140-2 certified algorithm, which is 128-bit or higher, such as Advanced Encryption Standard (AES); full disk encryption is recommended.
- VI.** The Provider/Representative agrees to pay the following fees associated with the use of the POS Network:
- A. For eligibility transactions, including Share of Cost clearance and Medi-Service reservations submitted through Medi-Cal-provided phone lines, there will be no transaction fee.
  - B. For Provider and/or Representative submission of pharmacy claims transactions through Medi-Cal-provided phone lines, there will be a fee of \$ .10 per approved claim transaction. An approved claim transaction is defined as a service, medical supply, durable medical equipment or drug supply that is determined to be payable through the claims adjudication process of the POS Network. This fee will be withheld from your regular Medi-Cal claims payment.
  - C. Any claim and/or eligibility transaction submitted on the Medi-Cal website will not have a transaction fee.
  - D. If the POS device is not being used over a reasonable amount of time, the Provider/Representative agrees to return the device. If the device is not returned in a timely manner, the Provider/Representative agrees to have the \$700 cost of the device deducted from future reimbursement.

**VII.**

Provider/Representative agrees, in order for the Provider/Representative's system to be activated for submission of actual Medi-Cal eligibility or claims-related transactions, to perform testing as required by DHCS and as documented in the *POS Network Interface Specifications* document or Medi-Cal website documents. Provider/Representative acknowledges that multiple tests may be required to activate the full functionality of the device/software/application and that all testing must be successfully concluded before the device/software/application will be activated.

**VIII.** Provider/Representative agrees to report all malfunctions of the POS Network or Medi-Cal website to Medi-Cal Fiscal Intermediary at the phone number and/or address listed below.

**IX.** Provider/Representative acknowledges that neither DHCS nor its agent is responsible for errors or problems, including problems of incompatibility, caused by hardware or software not provided by DHCS.

**X.** Provider/Representative acknowledges the attached Exhibit A---the BAA (Business Associate Addendum)--- and agrees to adhere to all privacy and security requirements within the BAA.

**XI. Provider or Non-Provider (Authorized Representative) Signature:**

I, the undersigned, am authorized and do attest and agree to all of the terms and conditions of this agreement.

\_\_\_\_\_  
Printed Name of Signee

\_\_\_\_\_  
Authorized Signature

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date

Address  
\_\_\_\_\_  
\\

CMC Submitter Number (if applicable): \_\_\_\_\_ N/A

**Please email the completed form to: [calaimjusticeprereleaseapps@dhcs.ca.gov](mailto:calaimjusticeprereleaseapps@dhcs.ca.gov). Please put "EVS Access" in the subject line of the email when submitting the form. Please allow ten business days for processing.**

**Exhibit A  
Business Associate  
Addendum**

1. This Agreement has been determined to constitute a business associate relationship under the Health Insurance Portability and Accountability Act (HIPAA) and its implementing privacy and security regulations at 45 Code of Federal Regulations, Parts 160 and 164 (collectively, and as used in this Agreement)
2. The term "Agreement" as used in this document refers to and includes both this Business Associate Addendum and the contract to which this Business Associate Agreement is attached as an exhibit, if any.
3. For purposes of this Agreement, the term "Business Associate" shall have the same meaning as set forth in 45 CFR section 160.103.
4. The Department of Health Care Services (DHCS) intends that Business Associate may create, receive, maintain, transmit or aggregate certain information pursuant to the terms of this Agreement, some of which information may constitute Protected Health Information (PHI) and/or confidential information protected by Federal and/or state laws.
  - 4.1 As used in this Agreement and unless otherwise stated, the term "PHI" refers to and includes both "PHI" as defined at 45 CFR section 160.103 and Personal Information (PI) as defined in the Information Practices Act at California Civil Code section 1798.3(a). PHI includes information in any form, including paper, oral, and electronic.
  - 4.2 As used in this Agreement, the term "confidential information" refers to information not otherwise defined as PHI in Section 4.1 of this Agreement, but to which state and/or federal privacy and/or security protections apply.
5. Contractor (however named elsewhere in this Agreement) is the Business Associate of DHCS acting on DHCS's behalf and provides services or arranges, performs or assists in the performance of functions or activities on behalf of DHCS, and may create, receive, maintain, transmit, aggregate, use or disclose PHI (collectively, "use or disclose PHI") in order to fulfill Business Associate's obligations under this Agreement. DHCS and Business Associate are each a party to this Agreement and are collectively referred to as the "parties."
6. The terms used in this Agreement, but not otherwise defined, shall have the same meanings as those terms in HIPAA. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.
7. **Permitted Uses and Disclosures of PHI by Business Associate.** Except as otherwise indicated in this Agreement, Business Associate may use or disclose PHI, inclusive of de-identified data derived from such PHI, only to perform functions, activities or services specified in this Agreement on behalf of DHCS, provided that such use or disclosure would not violate HIPAA or other applicable laws if done by DHCS.
  - 7.1 **Specific Use and Disclosure Provisions.** Except as otherwise indicated in this Agreement, Business Associate may use and disclose PHI if necessary for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate. Business Associate may disclose PHI for this purpose if the disclosure is required by law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware that the confidentiality of the information has been breached.

## **8. Compliance with Other Applicable Law**

- 8.1** To the extent that other state and/or federal laws provide additional, stricter and/or more protective (collectively, more protective) privacy and/or security protections to PHI or other confidential information covered under this Agreement beyond those provided through HIPAA, Business Associate agrees:
- 8.1.1** To comply with the more protective of the privacy and security standards set forth in applicable state or federal laws to the extent such standards provide a greater degree of protection and security than HIPAA or are otherwise more favorable to the individuals whose information is concerned; and
- 8.1.2** To treat any violation of such additional and/or more protective standards as a breach or security incident, as appropriate, pursuant to Section 18. of this Agreement.
- 8.2** Examples of laws that provide additional and/or stricter privacy protections to certain types of PHI and/or confidential information, as defined in Section 4. of this Agreement, include, but are not limited to the Information Practices Act, California Civil Code sections 1798-1798.78, Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2, Welfare and Institutions Code section 5328, and California Health and Safety Code section 11845.5.
- 8.3** If Business Associate is a Qualified Service Organization (QSO) as defined in 42 CFR section 2.11, Business Associate agrees to be bound by and comply with subdivisions (2)(i) and (2)(ii) under the definition of QSO in 42 CFR section 2.11.

## **9. Additional Responsibilities of Business Associate**

- 9.1 Nondisclosure.** Business Associate shall not use or disclose PHI or other confidential information other than as permitted or required by this Agreement or as required by law.

### **9.2 Safeguards and Security.**

- 9.2.1** Business Associate shall use safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI and other confidential data and comply, where applicable, with subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by this Agreement. Such safeguards shall be based on applicable Federal Information Processing Standards (FIPS) Publication 199 protection levels.
- 9.2.2** Business Associate shall, at a minimum, utilize an industry-recognized security framework when selecting and implementing its security controls, and shall maintain continuous compliance with its selected framework as it may be updated from time to time. Examples of industry-recognized security frameworks include but are not limited to
- 9.2.2.1** NIST SP 800-53 – National Institute of Standards and Technology Special Publication 800-53
- 9.2.2.2** FedRAMP – Federal Risk and Authorization Management Program
- 9.2.2.3** PCI – PCI Security Standards Council
- 9.2.2.4** ISO/IEC 27002 – International Organization for Standardization / International Electrotechnical Commission standard 27002
- 9.2.2.5** IRS PUB 1075 – Internal Revenue Service Publication 1075
- 9.2.2.6** HITRUST CSF – HITRUST Common Security Framework
- 9.2.3** Business Associate shall employ FIPS 140-2 compliant encryption of PHI at rest and in motion unless Business Associate determines it is not reasonable and appropriate to do so based upon



a risk assessment, and equivalent alternative measures are in place and documented as such. In addition, Business Associate shall maintain, at a minimum, the most current industry standards for transmission and storage of PHI and other confidential information.

**9.2.4** Business Associate shall apply security patches and upgrades, and keep virus software up-to-date, on all systems on which PHI and other confidential information may be used.

**9.2.5** Business Associate shall ensure that all members of its workforce with access to PHI and/or other confidential information sign a confidentiality statement prior to access to such data. The statement must be renewed annually.

**9.2.6** Business Associate shall identify the security official who is responsible for the development and implementation of the policies and procedures required by 45 CFR Part 164, Subpart C.

**9.3 Business Associate's Agent.** Business Associate shall ensure that any agents, subcontractors, subawardees, vendors or others (collectively, "agents") that use or disclose PHI and/or confidential information on behalf of Business Associate agree to the same restrictions and conditions that apply to Business Associate with respect to such PHI and/or confidential information.

**10. Mitigation of Harmful Effects.** Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI and other confidential information in violation of the requirements of this Agreement.

**11. Access to PHI.** Business Associate shall make PHI available in accordance with 45 CFR section 164.524.

**12. Amendment of PHI.** Business Associate shall make PHI available for amendment and incorporate any amendments to protected health information in accordance with 45 CFR section 164.526.

**13. Accounting for Disclosures.** Business Associate shall make available the information required to provide an accounting of disclosures in accordance with 45 CFR section 164.528.

**14. Compliance with DHCS Obligations.** To the extent Business Associate is to carry out an obligation of DHCS under 45 CFR Part 164, Subpart E, comply with the requirements of the subpart that apply to DHCS in the performance of such obligation.

**15. Access to Practices, Books and Records.** Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI on behalf of DHCS available to DHCS upon reasonable request, and to the federal Secretary of Health and Human Services for purposes of determining DHCS' compliance with 45 CFR Part 164, Subpart E.

**16. Return or Destroy PHI on Termination; Survival.** At termination of this Agreement, if feasible, Business Associate shall return or destroy all PHI and other confidential information received from, or created or received by Business Associate on behalf of, DHCS that Business Associate still maintains in any form and retain no copies of such information. If return or destruction is not feasible, Business Associate shall notify DHCS of the conditions that make the return or destruction infeasible, and DHCS and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI. If such return or destruction is not feasible, Business Associate shall extend the protections of this Agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

**17. Special Provision for SSA Data.** If Business Associate receives data from or on behalf of DHCS that was verified by or provided by the Social Security Administration (SSA data) and is subject to an agreement between DHCS and SSA, Business Associate shall provide, upon request by DHCS, a list of all employees and agents and employees who have access to such data, including employees and agents of its agents, to DHCS.

**18. Breaches and Security Incidents.** Business Associate shall implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and take the following steps:

**18.1 Notice to DHCS.**

**18.1.1** Business Associate shall notify DHCS **immediately** upon the discovery of a suspected breach or security incident that involves SSA data. This notification will be provided by email upon discovery of the breach. If Business Associate is unable to provide notification by email, then Business Associate shall provide notice by telephone to DHCS.

**18.1.2** Business Associate shall notify DHCS **within 24 hours by email** (or by telephone if Business Associate is unable to email DHCS) of the discovery of:

**18.1.2.1** Unsecured PHI if the PHI is reasonably believed to have been accessed or acquired by an unauthorized person;

**18.1.2.2** Any suspected security incident which risks unauthorized access to PHI and/or other confidential information;

**18.1.2.3** Any intrusion or unauthorized access, use or disclosure of PHI in violation of this Agreement; or

**18.1.2.4** Potential loss of confidential data affecting this Agreement.

**18.1.3** Notice shall be provided to the DHCS Program Contract Manager (as applicable), the DHCS Privacy Office, and the DHCS Information Security Office (collectively, "DHCS Contacts") using the DHCS Contact Information at Section 18.6 below.

Notice shall be made using the current DHCS "Privacy Incident Reporting Form" ("PIR Form"; the initial notice of a security incident or breach that is submitted is referred to as an "Initial PIR Form") and shall include all information known at the time the incident is reported. The form is available online at

<http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx>.

Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI, Business Associate shall take:

**18.1.3.1** Prompt action to mitigate any risks or damages involved with the security incident or breach; and

**18.1.3.2** Any action pertaining to such unauthorized disclosure required by applicable Federal and State law.

**18.2 Investigation.** Business Associate shall immediately investigate such security incident or confidential breach.

**18.3 Complete Report.** To provide a complete report of the investigation to the DHCS contacts within ten (10) working days of the discovery of the security incident or breach. This "Final PIR" must include any applicable additional information not included in the Initial Form. The Final PIR Form shall include an assessment of all known factors relevant to a determination of whether a breach occurred under HIPAA and other applicable federal and state laws. The report shall also include a full, detailed corrective action plan, including its implementation date and information on mitigation measures taken to halt and/or contain the improper use or disclosure. If DHCS requests information in addition to that requested through the PIR form, Business Associate shall make reasonable efforts to provide DHCS with such information. A "Supplemental PIR" may be used to submit revised or additional information after the Final PIR is submitted. DHCS will review and approve or disapprove Business

Associate's determination of whether a breach occurred, whether the security incident or breach is reportable to the appropriate entities, if individual notifications are required, and Business Associate's corrective action plan.

**18.3.1** If Business Associate does not complete a Final PIR within the ten (10) working day timeframe, Business Associate shall request approval from DHCS within the ten (10) working day timeframe of a new submission timeframe for the Final PIR.

**18.4 Notification of Individuals.** If the cause of a breach is attributable to Business Associate or its agents, Business Associate shall notify individuals accordingly and shall pay all costs of such notifications, as well as all costs associated with the breach. The notifications shall comply with applicable federal and state law. DHCS shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.

**18.5 Responsibility for Reporting of Breaches to Entities Other than DHCS.** If the cause of a breach of PHI is attributable to Business Associate or its subcontractors, Business Associate is responsible for all required reporting of the breach as required by applicable federal and state law.

**18.6 DHCS Contact Information.** To direct communications to the above referenced DHCS staff, the Contractor shall initiate contact as indicated here. DHCS reserves the right to make changes to the contact information below by giving written notice to Business Associate. These changes shall not require an amendment to this Agreement.

DHCS Program Contract Manager	DHCS Privacy Office	DHCS Information Security Office
See the Scope of Work exhibit for Program Contract Manager information. If this Business Associate Agreement is not attached as an exhibit to a contract, contact the DHCS signatory to this Agreement.	Privacy Office c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413  Email: <a href="mailto:incidents@dhcs.ca.gov">incidents@dhcs.ca.gov</a>  Telephone: (916) 445-4646	Information Security Office DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413  Email: <a href="mailto:incidents@dhcs.ca.gov">incidents@dhcs.ca.gov</a>

**19. Responsibility of DHCS.** DHCS agrees to not request the Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA and/or other applicable federal and/or state law.

## 20. Audits, Inspection and Enforcement

**20.1** From time to time, DHCS may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this Agreement. Business Associate shall promptly remedy any violation of this Agreement and shall certify the same to the DHCS Privacy Officer in writing. Whether or how DHCS exercises this provision shall not in any respect relieve Business Associate of its responsibility to comply with this Agreement.

**20.2** If Business Associate is the subject of an audit, compliance review, investigation or any proceeding that is related to the performance of its obligations pursuant to this Agreement, or is the subject of any judicial or administrative proceeding alleging a violation of HIPAA, Business Associate shall promptly notify DHCS unless it is legally prohibited from doing so.

## 21. Termination

**21.1 Termination for Cause.** Upon DHCS' knowledge of a violation of this Agreement by Business Associate, DHCS may in its discretion:

**21.1.1** Provide an opportunity for Business Associate to cure the violation and terminate this Agreement if Business Associate does not do so within the time specified by DHCS; or

**21.1.2** Terminate this Agreement if Business Associate has violated a material term of this Agreement.

**21.2 Judicial or Administrative Proceedings.** DHCS may terminate this Agreement if Business Associate is found to have violated HIPAA, or stipulates or consents to any such conclusion, in any judicial or administrative proceeding.

## **22. Miscellaneous Provisions**

**22.1 Disclaimer.** DHCS makes no warranty or representation that compliance by Business Associate with this Agreement will satisfy Business Associate's business needs or compliance obligations. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI and other confidential information.

### **22.2. Amendment.**

**22.2.1** Any provision of this Agreement which is in conflict with current or future applicable Federal or State laws is hereby amended to conform to the provisions of those laws. Such amendment of this Agreement shall be effective on the effective date of the laws necessitating it, and shall be binding on the parties even though such amendment may not have been reduced to writing and formally agreed upon and executed by the parties.

**22.2.2** Failure by Business Associate to take necessary actions required by amendments to this Agreement under Section 22.2.1 shall constitute a material violation of this Agreement.

**22.3 Assistance in Litigation or Administrative Proceedings.** Business Associate shall make itself and its employees and agents available to DHCS at no cost to DHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCS, its directors, officers and/or employees based upon claimed violation of HIPAA, which involve inactions or actions by the Business Associate.

**22.4 No Third-Party Beneficiaries.** Nothing in this Agreement is intended to or shall confer, upon any third person any rights or remedies whatsoever.

**22.5 Interpretation.** The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA and other applicable laws.

**22.6 No Waiver of Obligations.** No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

DHCS' Eligibility Verification System (EVS):  
User Guide for Pre-Release Medi-Cal Application Processes (Enclosure #2)

This document is intended to provide County Correctional Facilities and County Youth Correctional Facilities (CCFs), and/or their designated entity or entities with information on how to use the Department of Health Care Services' (DHCS) Eligibility Verification System (EVS) to verify whether an incarcerated individual is currently enrolled in Medi-Cal. If the individual is not enrolled in Medi-Cal, and wishes to apply, CCFs or their designated entity would assist the individual with completing and submitting a Medi-Cal application.

The EVS has three methods available for verifying Medi-Cal enrollment:

- Internet Eligibility Verification (Medi-Cal Provider website)
- Third Party Software (contact CMC Help Desk at 1-800-541-5555)
- Automated Eligibility Verification System (AEVS) via 1-800-456-2387

### Background Information Related to Medi-Cal Eligibility

#### **Benefits Identification Card**

The Department of Health Care Services (DHCS) issues a plastic Benefits Identification Card (BIC) to each Medi-Cal enrollee. The BIC includes a nine-character Client Identification Number (CIN), a check digit and a four-digit date that matches the date of issue.<sup>1</sup> These data can be entered into the Eligibility Verification System network to determine if an individual is currently enrolled in Medi-Cal and if so, their scope of benefits. Note that it is more likely that the correctional facility will use other data (e.g., SSN) to look up an individual in EVS.

#### **Temporary Paper BIC**

In some cases, (e.g., when an individual is a short-term stay and is released from a CCF before a plastic card can be issued), recipients are issued temporary paper Medi-Cal BIC cards from either the County Welfare Department (CWD) or a Presumptive Eligibility Provider. The card contains a 14-digit ID number and is used like a plastic BIC. Temporary paper identification cards can be issued for the following reasons:

- Recipients new to Medi-Cal who have an immediate need for health care services
- Recipients currently eligible for Medi-Cal who have an immediate need for replacement ID cards

#### **Eligibility Verification Terminology**

The terminology used within the EVS processes may differ slightly from the terminology used within the CCFs or designated entity.

<b>Eligibility Verification System Terminology</b>	<b>Definition or Application to CCF/Designated Entity</b>
Subscriber Birth Date	Individual's Date of Birth
Issue Date	Individual's BIC Issue Date

---

<sup>1</sup> The BIC issue date is used to deactivate a card when reported as lost or stolen.

DHCS' Eligibility Verification System (EVS):  
User Guide for Pre-Release Medi-Cal Application Processes (Enclosure #2)

<b>Eligibility Verification System Terminology</b>	<b>Definition or Application to CCF/Designated Entity</b>
Service Date	Date in which enrollment is verified
Trace Number (Eligibility Verification Confirmation [EVC] Number)	Confirmation number to be used as evidence of enrollment verification
Subscriber First Name	Individual's First Name
Subscriber Last Name	Individual's Last Name
Medical Services Reservation	<i>Not Applicable for Pre-Release Application purposes</i>
Medicaid Provider Number	<i>Not Applicable for Pre-Release Application purposes</i>
Subscriber	Recipient
Subscriber ID	Recipient ID
Spend Down Amount (or SOC)	<i>Not Applicable for Pre-Release Application purposes</i>
Subscriber ID	Individual's BIC ID Number, Client Identification Number (CIN), or Social Security Number

**Data Elements Required for Medi-Cal Enrollment Verification**

In order to verify an individual's Medi-Cal enrollment, a few key pieces of information is **required** about the individual:

<b>Related Internet Eligibility Verification field:</b>	<b>Required information about the individual:</b>
Subscriber ID number	Individual's BIC ID Number, Client Identification Number (CIN), or Social Security Number*
Subscriber Date of Birth (DOB)	Individual's Date of Birth
BIC Issue date	Individual's BIC Issue Date- if unknown, or searching by SSN, please <u>use the current date</u>
Date of Service (DOS)	Today's date or a date within one year prior Note: Cannot be a future date.

\*If the CCFs or their designated entity does not have the individual's SSN, the local CWD would need to provide eligibility verification of that individual. The CCFs or the designated entity should provide the CWD with applicable information to properly identify the individual.

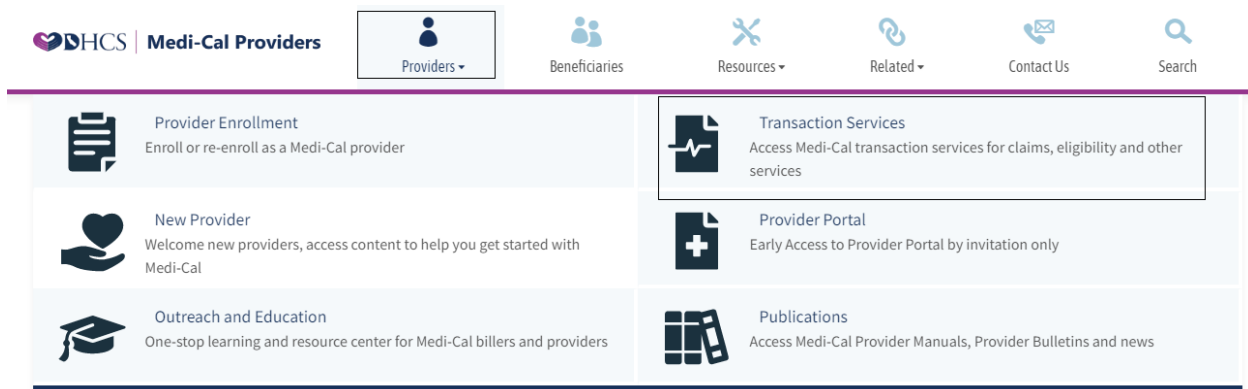
# DHCS' Eligibility Verification System (EVS): User Guide for Pre-Release Medi-Cal Application Processes (Enclosure #2)

## Internet Eligibility Verification using the Medi-Cal Provider Website **Website Access Requirements**

- Complete and submit Medi-Cal POS Network/Internet Agreement form
- Receive Medi-Cal Provider website User ID and a PIN

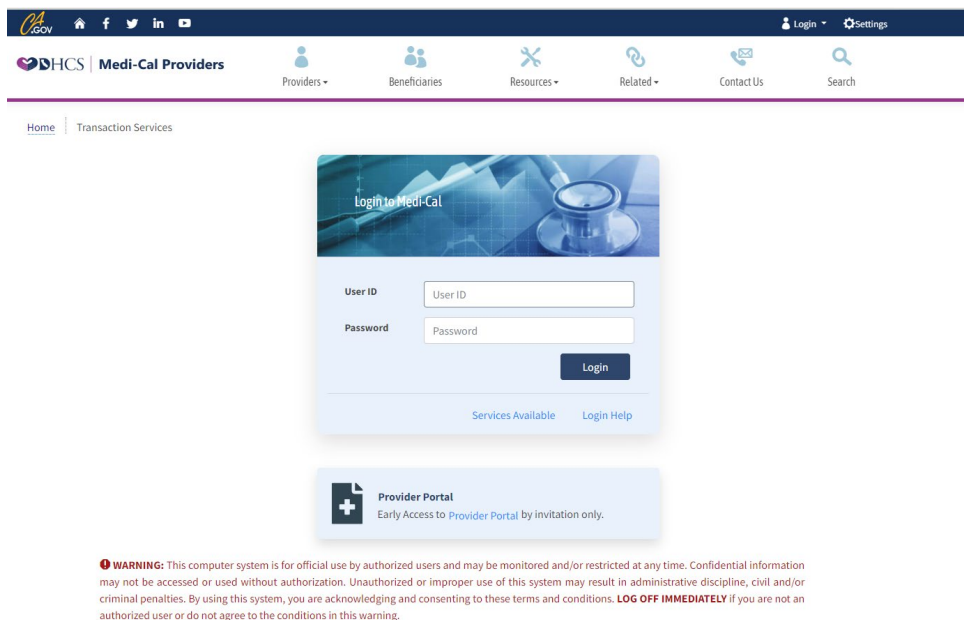
To perform an internet eligibility verification:

1. Login to the Medi-Cal Provider website: <https://www.medi-cal.ca.gov/>
2. From the Provider drop-down menu, select **Transaction Services**.



*Medi-Cal Provider drop-down menu.*

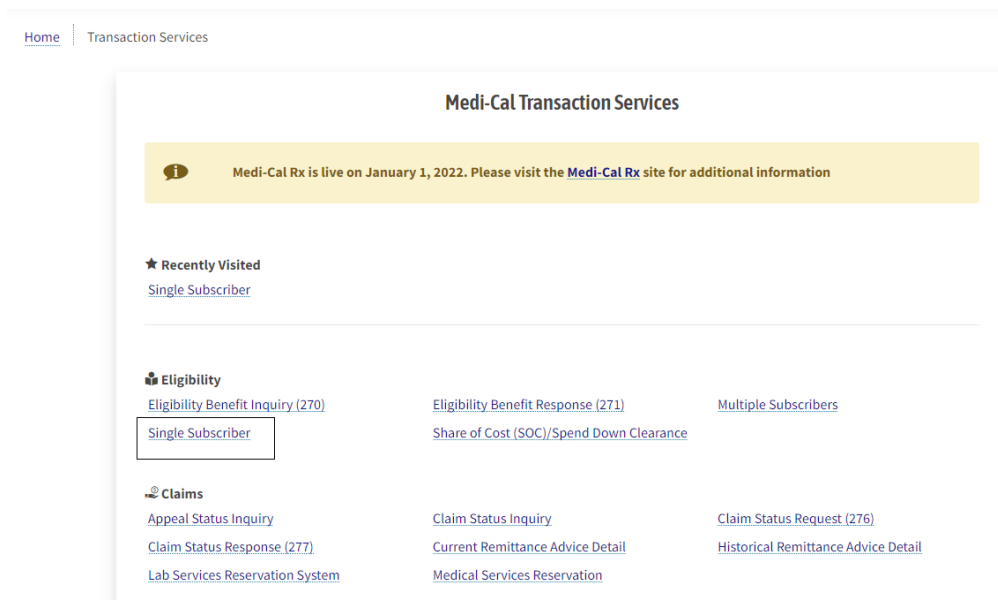
3. Login to Transaction Services with your User ID and PIN.



*Transaction Services Login Page*

# DHCS' Eligibility Verification System (EVS): User Guide for Pre-Release Medi-Cal Application Processes (Enclosure #2)

## 4. Select **Single Subscriber**.



*Medi-Cal Transaction Services page – Single Subscriber link*

## 4. Fill out the **Single Subscriber** form and select **Submit**.

The screenshot shows the 'Single Subscriber' form. The form is titled 'Single Subscriber' and has a sub-header 'Single Subscriber Eligibility'. A red asterisk indicates required fields. The form contains three main sections: 'Subscriber ID' with a text input field, 'Subscriber Birth Date' with a date picker (mm/dd/yyyy), and 'Issue Date' with a date picker (mm/dd/yyyy). There is also a 'Service Date' field with a date picker (mm/dd/yyyy). A 'Submit' button is located at the bottom right of the form. The background shows the DHCS website navigation menu with links for 'Providers', 'Beneficiaries', 'Resources', 'Related', 'Contact Us', and 'Search'.

*Single Subscriber form*



DHCS' Eligibility Verification System (EVS):  
User Guide for Pre-Release Medi-Cal Application Processes (Enclosure #2)

### Eligibility Responses and Required Action

After searching for the individual, an eligibility response will be displayed. The eligibility information is displayed, along with a green, yellow, or red banner. The color and the eligibility message should be used together to determine what next steps are necessary for pre-release application process.

It is important to confirm the name and other information about the individual on the response match the individual whose eligibility being verified. If it does not, the eligibility information reported should not be used.

#### **GREEN BANNER**

The green banner at the top of the page (with a check mark inside a circle) means Medi-Cal enrollment is established for the individual on that specific date of service. It also means that providers may render Medi-Cal services.

#### **Example of Active Medi-Cal Benefits:**

Single Subscriber Response

Eligibility transaction performed by provider: on Wednesday, January 12, 2022 at 11:36:44 AM

✓ Eligibility Message: SUBSCRIBER LAST NAME: . EVC #: 901J9V7MM9. CNTY CODE: 02. PRMY AID CODE: 60. MEDI-CAL ELIGIBLE W/ NO SOC/SPEND DOWN.

Name:	Subscriber ID:
Service Date: 12/01/2021	Subscriber Birth Date:
Issue Date: 03/08/2013	Primary Aid Code: 60
First Special Aid Code:	Second Special Aid Code:
Third Special Aid Code:	Subscriber County: 02-Alpine
HIC Number:	
Trace Number (Eligibility Verification Confirmation (EVC) Number): 901J9V7MM9	

*Eligibility Message with green banner*

Required Action: This individual is enrolled in Medi-Cal and a Pre-Release Medi-Cal Application is **not** needed. However, the CCFs or their designated entity **must work** with the local CWD to verify that they have the accurate demographic and incarceration information (incarceration date and expected release date if known) on file for the individual.

#### **YELLOW BANNER**


The yellow banner at the top (with an exclamation point [!] inside a triangle) indicates the individual's special circumstances, such as the individual is reported as incarcerated with an active suspension of benefits, has limited coverage, or has other case restrictions. The Eligibility message is an important part of determining what action is required.

DHCS' Eligibility Verification System (EVS):  
User Guide for Pre-Release Medi-Cal Application Processes (Enclosure #2)

**Active Suspension of Medi-Cal Benefits due to Incarceration:**

Single Subscriber Response

Eligibility Transaction Performed by: on Friday, February 17, 2023 at 8:52:44 AM

 **Eligibility Message:** SUBSCRIBER LAST NAME: . SUBSCRIBER REPORTED AS INCARCERATED, CONTACT COUNTY WELFARE AGENCY FOR MORE INFORMATION.

Subscriber Name:	Subscriber ID:
Subscriber Birth Date:	Issue Date: 10/18/1993
Primary Aid Code:	First Special Aid Code:
Second Special Aid Code:	Third Special Aid Code:
Responsible County: -unknown	Medicare ID:
Service Date: 01/01/2023	Trace Number/Eligibility Verification Confirmation Number:


*Eligibility Message with yellow banner*

Required Action: This individual is enrolled in Medi-Cal and their Medi-Cal benefits are suspended due to being incarceration. A Pre-Release Medi-Cal Application is **not** needed for this individual because they have Medi-Cal. However, the CWDs or their designated entity **must work** with the local CWD to verify that they have the accurate demographic and incarceration information (incarceration date and expected release date if known) on file for the individual.

**Medi-Cal Inmate Eligibility Program (MCIEP) Eligibility:**

Single Subscriber Response

Eligibility Transaction Performed by: on Thursday, February 16, 2023 at 4:30:27 PM

 **Eligibility Message:** SUBSCRIBER LAST NAME: . EVC #: 557KWMKPZM. CNTY CODE: 33. 1ST SPECIAL AID CODE: N5. MEDI-CAL ELIGIBLE LIMITED TO SERVICES PROVIDED ONLY IN AN INPATIENT HOSPITAL FACILITY.

Subscriber Name:	Subscriber ID:
Subscriber Birth Date:	Issue Date: 05/04/2005
Primary Aid Code:	First Special Aid Code: N5
Second Special Aid Code:	Third Special Aid Code:
Responsible County: 33-Riverside	Medicare ID:
Service Date: 01/23/2023	Trace Number/Eligibility Verification Confirmation Number: 557KWMKPZM

*Eligibility Message with yellow banner*

Required Action: This individual is enrolled in the Medi-Cal Inmate Eligibility Program. Inmate aid codes take precedence over other Medi-Cal aid codes, which prevents any other eligibility from being displayed. CCFs or their designated entity **must work** with

DHCS' Eligibility Verification System (EVS):  
User Guide for Pre-Release Medi-Cal Application Processes (Enclosure #2)

the local CWD to determine if a Pre-Release Medi-Cal Application is needed and to verify that the CWD has the accurate demographic and incarceration information (incarceration date and expected release date if known) on file for the individual.

**Limited or Restricted Coverage:**

Single Subscriber Response

**Eligibility transaction performed by provider:** on Wednesday, January 12, 2022 at 4:29:18 PM

**Eligibility Message:** SUBSCRIBER LAST NAME: . EVC #: 2119P79W1Q. CNTY CODE: 02. PRMY AID CODE: 84. 2ND SPECIAL AID CODE: 7H. AID CODE NO LONGER IN USE. CALL ADVANCED MEDICAL MANAGEMENT 1-877-589-6807. MEDI-CAL ELIGIBLE FOR O/P TUBERCULOSIS RELATED SVCS W/ NO SOC/SPEND DOWN. OTHER HEALTH INSURANCE COV UNDER CODE A.

<b>Name:</b>	<b>Subscriber ID:</b>
<b>Service Date:</b> 10/01/2021	<b>Subscriber Birth Date:</b>
<b>Issue Date:</b> 10/18/1993	<b>Primary Aid Code:</b> 84
<b>First Special Aid Code:</b>	<b>Second Special Aid Code:</b> 7H
<b>Third Special Aid Code:</b>	<b>Subscriber County:</b> 02-Alpine
<b>HIC Number:</b>	
<b>Primary Care Physician Phone #:</b>	<b>Service Type:</b>
<b>Trace Number (Eligibility Verification Confirmation (EVC) Number):</b> 2119P79W1Q	

*Eligibility Message with yellow banner*

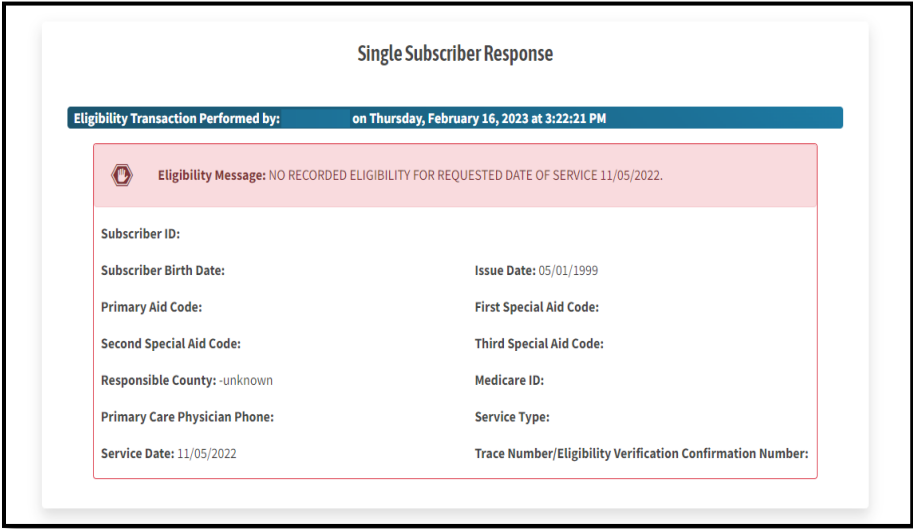
Required Action: This individual is enrolled in Medi-Cal and a Pre-Release Medi-Cal Application is **not** needed, but the CCF or their designated entity **must work** with the CWD to verify that the CWD has the accurate demographic and incarceration information (incarceration date and expected release date if known) on file for the individual.

**RED BANNER**

The red banner at the top (with a hand inside a hexagon) means there is no Medi-Cal enrollment established for the individual on that specific date of service.

**Not Currently Enrolled:**

DHCS' Eligibility Verification System (EVS):  
User Guide for Pre-Release Medi-Cal Application Processes (Enclosure #2)



Single Subscriber Response

Eligibility Transaction Performed by: on Thursday, February 16, 2023 at 3:22:21 PM

**Eligibility Message:** NO RECORDED ELIGIBILITY FOR REQUESTED DATE OF SERVICE 11/05/2022.

Subscriber ID:	
Subscriber Birth Date:	Issue Date: 05/01/1999
Primary Aid Code:	First Special Aid Code:
Second Special Aid Code:	Third Special Aid Code:
Responsible County: -unknown	Medicare ID:
Primary Care Physician Phone:	Service Type:
Service Date: 11/05/2022	Trace Number/Eligibility Verification Confirmation Number:

*Eligibility Message with red banner*

Required Action: CCFs or their designated entity **should work with the individual to complete a Pre-Release Medi-Cal application**, since the individual is not already enrolled in Medi-Cal.

### **Batch Eligibility Requests and Responses**

For information about how to establish batch eligibility requests of up to 99 individual records, please contact DHCS at [CalAIMJusticePreReleaseApps@dhcs.ca.gov](mailto:CalAIMJusticePreReleaseApps@dhcs.ca.gov).