DHCS
CALIFORNIA DEPARTMENT OF
HEALTH CARE SERVICES
Michelle Baass | Director

DATE: June 8, 2023

Medi-Cal Eligibility Division Information Letter No.: I 23-35E

TO: ALL COUNTY WELFARE DIRECTORS
ALL COUNTY ADMINISTRATIVE OFFICERS
ALL COUNTY MEDI-CAL PROGRAM SPECIALISTS/LIAISONS
ALL COUNTY PRIVACY AND SECURITY OFFICERS

SUBJECT: ERRATA TO MEDI-CAL ELIGIBILITY DIVISION INFORMATION LETTER NO. 23-35: REMOTE WORK POLICY FOR THE USE OF MEDI-CAL PERSONALLY IDENTIFIABLE INFORMATION (PII) WHILE WORKING REMOTELY.

The purpose of this Medi-Cal Eligibility Division Information Letter (MEDIL) errata is to provide counties with an updated Enclosure of MEDIL I 23-35, DHCS Remote Work Policy to reflect changes to the encryption requirements. Guidance in this letter takes effect immediately.

Corrections to the Enclosure of MEDIL I 23-35 are recorded using the following:

- ~~strike-through~~ for deleted language
- **underline and bolding** for adding new language

Below is the language from MEDIL I 23-35, with the revisions located on page 1 of the Enclosure.

- ~~FIPS 140-3 compliant end-to-end encryption;~~ **FIPS 140-2 or greater approved security functions as described in section 6.2.2 of NIST SP 800-140Cr1;**

If you have any questions, or if we can provide further information, please contact DHCS' Privacy and Security Team, by email at CountyPSA@dhcs.ca.gov.

Sincerely,

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

Remote Work Policy

This guidance is effective May 12, 2023, and applies to users of the DHCS' Medi-Cal Eligibility Data System (MEDS) and MEDSLITE system or County Welfare Departments/Agencies that use Medi-Cal Personally Identifiable Information (PII) while working remotely.

Remote Access Requirements

To facilitate the essential work that is supported by MEDS, MEDSLITE, and Medi-Cal PII, the guidelines listed below must be followed for remote access when Medi-Cal PII is accessed remotely. For the purposes of this policy, "working remotely" means working from a physical location not under the control of the person's employer. DHCS requests that entities access systems storying Medi-Cal PII only through a secure remote access solution that includes, at a minimum, the following to reduce the associated risks:

- ~~FIPS 140-3 compliant end-to-end encryption;~~ **FIPS 140-2 or greater approved security functions as described in section 6.2.2 of NIST SP 800-140Cr1;**
- Multi-Factor Authentication (MFA) using methods such as a One-Time Passcode (OTP), Mobile authenticator app, security token or at minimum a device certificate;
- Audit trails and logs of remote access that are kept for at least one year;
- If users are authorized to access MEDS or MEDSLITE from a personal device through Citrix or VDI technology, data must not be stored, copied, or sent to personal devices. Technology, such as but not limited to containerization, virtual desktop infrastructure (VDI), Citrix etc., are required to prevent data leakage to personal devices;
- Corporate issued devices should leverage Virtual Private Network (VPN) technology that includes MFA for remote access to MEDS or MEDSLITE.
- Remote access or telework policies and procedures, including but not limited to using physical isolation or barriers to prevent other home occupants from seeing confidential data from these systems.

Data protection

Information security is a set of practices designed to keep personal and confidential data secure from unauthorized access, disclosures, or modifications during the storage or transmission of data, which can be in the form of electronic or physical media. Sections 6 – 6.6 and 7.4 of SIMM 5360-A, Telework and Remote Access Security Standard provides more information on maintaining the security of information assets used for Telework.

- Protect information assets (physical or electronic) from unauthorized access and use by others. Do not disclose confidential or sensitive data to any unauthorized personnel, including family members, friends, and other visitors.

- Do not store State of California sensitive or confidential information on your personal computer.
- Do not use personal email for business use, and do not use business-issued email for personal use.
- Assign a strong passcode to lock/unlock mobile devices.
- Always lock your mobile or computing device when not in use.
- Ensure websites are encrypted (look for “https” in your web browser address bar) when working with sensitive data.
- Become familiar with your department’s procedures for reporting a security incident of a lost or stolen mobile or computing device.
- Report security concerns or incidents to management immediately.
- Always comply with your organization’s policies and procedures to protect specific high-risk data elements regulated by HIPAA, IRS, PCI, etc.
- Secure information assets (physical or electronic) by storing them only in secured locations (e.g., locked cabinets or drawers, locked rooms in locked buildings), as applicable.
- Store any sensitive or confidential information on encrypted media provided by your agency or department.
- Never download or copy state data without authorization
- Never download or copy state data to an unencrypted portable media device.
- Ensure confidential paper documents are properly disposed of, i.e., shredding.

Passwords

Security best practice strongly recommends using a passphrase, or string of words, to increase the length of your password. The best passphrases are easy for you to remember but, because of length, more difficult to crack. The following is recommended when creating your passphrase:

- Make it easy to remember.
- Make it long enough to be hard to guess, a minimum of 15 characters.
- Make it hard to guess by intuition, even by someone who knows you well.
- Do not use famous quotations.
- Do not include personal information such as your name or pets’ names.
- Passwords should include at least one number. Passwords with more than one number must be non-repeating or non-consecutive (e.g., 555, 1234).
- Substitute letters with numbers and punctuation marks or symbols.
- Examples:
    - 3Chicagochilidogsplease!
    - Thedogissleepingsoundly2night
    - Uhaventlikedhotsauceincoffeesince1989!
    - Wouldyoulikeasandwichin10minutes?

Always use a unique password for each account. It is risky to use the same password for multiple accounts.

Privacy

State government collects and utilizes large amounts of confidential and personal data and is responsible for safeguarding and protecting that data.

- Only use personal information required to perform specific business function(s).
- Practice effective Information Handling Practices such as Principle of Least Privilege (PoLP) to help safeguard confidential and personal data.
- If confidential or personal data is shared, conduct due diligence, and maintain oversight of partners and vendors.
- If someone provides services on your behalf, you are responsible for how they collect, use, and secure the confidential or personal data.
- Know the department's privacy and security policies, stay informed, and follow them.

Physical Security

- Consider the use of additional physical security controls, such as locking the telework device to a stationary object (e.g., desk or chair) with a computer cable lock, where appropriate.
- Ensure confidential paper documents are properly disposed of (i.e., shredding).
- Do not leave information assets unattended in vehicles or other locations where they may be easily stolen.
- Do not write down or share passwords with anyone.

Wi-Fi Protection

- Turn off unnecessary services like Bluetooth, unused Wi-Fi, etc.
- Protect your home Wi-Fi with a password. Protect your device with a password.
- Do not connect to public or untrusted/insecure Wi-Fi connections.
- Follow Center for Internet Security (CIS) recommendations for securing home networks
  - https://www.cisecurity.org/insights/newsletter/how-to-secure-your-home-network-against-cyber-threats

Secure your personal network

Ensure your own information assets are configured to limit network access, including:

- Make sure your firewall is turned on.
- Disable services and features that you are not using.
- Configure information assets so that they do not automatically attempt to join wireless networks they detect.

Teleconference security tips

- Do not share or advertise your meeting link publicly.
- Set a strong password for all teleconference meetings hosted (e.g., $yBerT@k8s!1), and do not reuse passwords.
- Refrain from discussing sensitive topics or sharing documents with confidential or personal data.
- Lock the meeting once all attendees have joined. Verify and remove any unknown participants who dialed in before you start the meeting.

- Do not use your personal or other non-department teleconferencing accounts to host work-related meetings.
- Manage screen-sharing options by limiting this ability to only the host, and never allow others to take control of your screen/device.
- Be cautious of what is visible within the camera range and on screen.
- Take notice if a meeting you attend is being recorded. Ensure verbal consent is given by all parties before recording a meeting.
- Refrain from downloading shared files and/or documents onto personal devices.
- Ensure that sensitive and legal communication is conducted through a FedRAMP-compliant teleconferencing tool.

If an entity whose staff use Medi-Cal PII remotely is unable to perform essential work in compliance with these standards, the entity will be subjected to an ongoing Plan of Action and Milestones (POA&M), detailing a concrete roadmap to becoming fully compliant. This POA&M must be provided to DHCS for review and approval. Any entities under a POA&M will be required to provide quarterly updates to DHCS until the fully compliant. DHCS reserves the right to limit or prohibit telework access to MEDS and MEDSLITE as conditions warrant.

Please submit any questions to CountyPSA@dhcs.ca.gov.