K. Management Information System

The County of San Diego BHS manages an electronic health record (EHR) for the BHP County and Contracted providers. An electronic health record (EHR) will replace much of what is contained in the hybrid medical record. Many controls are built into the software and hardware to safeguard the security and privacy of member personal health information. The electronic Mental Health Management Information System (MH MIS) utilized by the BHP is Streamline SmartCare. All member information, including clinical documentation, is entered into SmartCare allowing for improved coordination of care across the BHP System of Care. For documentation and user guidance, please reference the CalMHSA Website and the to the Optum Website ('*SmartCare'* tab and '*UCRM'* tab).

SmartCare

User Account Setup and Access

SmartCare Software is a web-based application that is managed by CalMHSA. Access to SmartCare is through a secure portal which requires a user to establish an account in which you must obtain an identification number, menu group, and password. Access to SmartCare is granted through the MIS Unit by completing the appropriate access and security forms.

System Administration for SmartCare is shared between the Administrative Services Organization (ASO) and the County's MIS Unit. The ASO is responsible for other system administration activities such as table management, system maintenance, updates to the application, managing SmartCare environments, producing reports for legal entities, electronic submission of state reporting, coordination with SmartCare Software, and providing the User Support Help Desk (for access issues).

The Mental Health Management Information System (MH MIS) is used by County and contract operated programs for member tracking, managed care functions, reporting and billing. The MIS Unit is responsible for managing access, security, and menu management in SmartCare in accordance with County, State and Federal HIPAA regulations. The MIS Unit is also the gatekeeper who ensures that staff is only given access pursuant to contract agreements. In addition, the MIS Unit is responsible for coordination among the County Technology Office, SmartCare and the ASO.

Technical Requirements to Access SmartCare

Prior to accessing the SmartCare application via the internet, there are some basic technical requirements. For questions about whether an individual user or program site

meets the basic technical requirements, it is recommended that the individual or program contact their company's IT department. The ASO may also be able to provide some technical assistance. Additional support regarding SmartCare's hardware, software and network requirements can be found on the Optum Website.

Staff Set Up and User Account Access

All individuals who provide services or perform some other activity to be recorded SmartCare as well as those who are authorized to access SmartCare must have a staff account. A "staff" in SmartCare is defined as an individual who is employed, contracted or otherwise authorized by his or her designated legal entity or County business group to operate within the County of San Diego public behavioral health System of Care and whose primary job function may include any one of the following: to provide Behavioral Health Services, Quality Assurance activities, enter data, view data, or run reports. This includes clinicians, doctors, nurses, office support staff, financial/billing staff, research/analyst staff and program managers/administrative staff. All Staff providing services must provide National Provider Identifier (NPI) and taxonomy numbers. All staff will be assigned a username.

User Access requires the following steps:

1. Program manager completes the "SmartCare Access Request Form" (ARF) located on the Optum Website> SmartCare tab.

2. All new users must successfully complete the required SmartCare Training Modules after creating a CalMHSA LMS Account.

3. Contractor employee and employee's supervisor must read and sign the "Staff Electronic Signature Agreement".

4. Contractor employee and employee's supervisor must also read and sign the County's "Summary of Policies" (SOP) form.

5. Email all completed forms to:

MIS Unit
BHSEHRAccessRequest.HHSA@sdcounty.ca.gov
and BHSCredentialing@optum.com

All forms **must** be typed and contain all necessary information. Incomplete forms will be returned to the contact person listed on the form. Once completed correctly, the forms must be resubmitted to the MIS Unit. Please ensure forms are completed correctly to avoid delay in user account setup. All forms with instructions are available electronically on the ASO's (Optum) Public Sector website.

Once all forms have been submitted, the MIS Unit will set up SmartCare User Account with username and password. The user will be provided his/her username and password after completing required trainings. Program managers and other supervisors are responsible for registering new staff who will be users to attend the SmartCare training and confirming that employees have successfully completed SmartCare training.

Staff Assignment to Programs

Staff are given access to specific programs based upon the program(s) where they work. Staff are also given access to specific menus based on their respective job functions. A list and definition of menus is available on the Request Form. Staff authorized to access SmartCare will be given login access and a password and are considered "users". Staff may be assigned to a single or multiple programs. The programs must be reflected on the SmartCare Account Request Form (ARF) completed by the program manager.

The MIS Unit will monitor staff access to programs to ensure that staff has been assigned correctly. Under no circumstances should a staff be assigned to a CDAG or program if that staff person does not perform work for that program. This would constitute a violation of security and member confidentiality.

User Assignment to a Clinical Data Access Group (CDAG)

Each user is granted restricted access to MH MIS based on his/her job requirements. One of the ways that access is restricted is through assignment to programs described above. Access is further restricted by assignment to a clinical data access group or CDAG. A CDAG defines the screens and reports the user will be able to access and whether the user can add/edit or delete for each of those screens. For example, the user may only be able to view but not change data in one screen but may have rights to add data or edit previously entered data for another screen. CDAG groups are created based on multiple criteria such as security, level of access to member information, staff job functions, staff credentials and state and federal privacy regulations.

On the ARF, the program manager or supervisor is responsible for requesting the CDAG assignment for each user based on his/her job functions. A user may only be in one CDAG group at a time. Therefore, it is important for the program manager/supervisor to determine which CDAG group is the best match for the job functions performed by his/her staff. If a person is employed by more than one legal entity, he/she may have different CDAG assignments. The provider will have to select the correct CDAG upon login to SmartCare.

For example, there will be Roles for:

- Data entry staff with full member look up rights
- Data entry staff with limited member look up

- Clinicians
- Program managers and supervisors
- Quality Assurance
- Billing staff
- Billing only (For Billing Purposes Only – It has no views)
- Research and Analysts

Refer to the ARF Instructions for a list and definition of available menus. The MIS Unit will review role group requested by the program manager/supervisor and approve or modify the request.

Guidelines when the EHR is Unavailable

Programs are expected to adhere to County and Medi-Cal Documentation standards, even on occasions when the EHR is temporarily out of operation. When an unplanned disruption occurs, programs will receive an email alert from the CalMHSA Helpdesk. Consider the circumstances and apply best judgement to determine if it is prudent to use paper methods for documentation of services. Review UCRM to determine if the documentation/data is required to be entered manually into the EHR or can be scanned into the EHR/maintained in paper format in the Hybrid Chart. Paper billing records should be given to administrative staff for later entry in the EHR. Services may be claimed after documentation on paper notes or signature in the EHR.

It is strongly recommended that programs Save and Sign documentation as soon as possible within the stated timelines, in order to avoid risk of late entry and being out of compliance. Continued problems with the EHR should be reported directly to the CalMHSA Helpdesk.

Questions about the documentation process may be sent to: QImatters.hhsa@sdcounty.ca.gov.

SmartCare for Prescribers

CalMHSA Rx

Prescribers, and nurses who stage medications for prescribers, will have access to CalMHSA Rx. Prescribers who need to be set up to electronically prescribe controlled substances (EPCS) must additionally go through an identity proofing process and a soft or hard token must be established within their account. Both primary and backup tokens are required in SmartCare. Behavioral Health Services (BHS) will implement a new electronic prescribing (e-prescribing) component with the SmartCare go-live called CalMHSA Rx (previously DrFirst). CalMHSA Rx uses a medication management

software called Rcopia that will seamlessly integrate with SmartCare for e-prescribing, meaning no additional login will be required. Doctors who will use SmartCare to e-prescribe will use CalMHSA Rx. For a step-by-step guide, including the information needed for identity verification, please see the EPCS Invite Guide at: Optum Website> SMH & DMC-ODS- Health Plans> SmartCare> *Training* .

Other Resources for Prescribers

- CalMHSA Home Page > *Prescriber Documentation* and *CalMHSA Rx*
- SmartCare DrFirst Guidance (additional information re. hard and soft tokens)
- Quick Start for CalMHSA RX Users

User Support

Users can obtain support through the CalMHSA HelpDesk. The CalMHSA HelpDesk can assist a user with the MH MIS application (technical assistance), MH MIS password issues, connectivity/access problems, printer problems, data entry questions, special requests, such as reports for contractors.

- SmartCare support for system issues is offered by CalMHSA during normal business hours (M-F 8am-5pm)
- Connect via Live Chat at or Submit a Ticket
- Register for a Customer Ticket Portal Account
- After normal business hours the only support available is for system outages. You can call (916) 214-8348

Numerous SmartCare resources are available to assist you with workflow and documentation questions:

1. Go to the CalMHSA Website
2. Access help from within SmartCare
    a. Once you are logged in to SmartCare, you can access help in the following ways:
        i. Use the CalMHSA AI Documentation chatbot to ask direct questions about workflow and documentation

ii. Click on the black question mark at the bottom of your screen to find “how to” documents on the CalMHSA website.

3. Access San Diego Specific Resources

   a. For resources and guidance specific to San Diego County’s use of SmartCare, go to either the BHP Provider Documents or Organized Delivery System Drug Medi-Cal pages of the Optum website> *SmartCare* tab.

Security and Confidentiality

The County of San Diego is responsible for the protection of County technology and data and to monitor through its own policies and procedures user compliance with state and federal privacy and confidentiality regulations. The County’s Security mandates state that access will be given to a user at the least minimum level required by the user to execute the duties or job functions and that only those individuals with a “need to know” will be given access. Protection of County data and systems is also achieved via the use of unique user identification and passwords as well as other tracking methods.

Limitation of Staff Assignment to “Data Entry – Add New Clients”

Program staff will be allowed to view information about a member currently or previously served by their program. Designated program staff will be given access to the “full client look up” to add new members and assign existing members to their program. These individuals will be allowed to view all members in the system, including those not served by their program. This access allows for data entry, adding new members, full client lookup; entering demographic, diagnosis, insurance, and financial information (UMDAP); opening assignments; and running reports.

Program Manager/Supervisor Responsibility for Staff Access

The program manager/supervisor shall ensure that staff are in compliance with all County, State and Federal privacy and confidentiality regulations regarding security, providers protected health information (PHI). In addition, the program manager shall ensure that their staff are aware of the County’s Security Policy regarding the protection of network/application passwords and use of County systems and data as outlined in San Diego County’s “Summary of Policy”. The program manager shall immediately notify the MIS Unit whenever there is a change in information such as staff demographics, email, job title, credential/licensure, and jobs, or are program assignment. This includes the initial staff setup, modifying or terminating existing staff accounts**.**

Under no circumstances shall a staff person who has terminated employment have access to the EHR through SmartCare. This would constitute a serious violation of security which may lead to disciplinary actions.

Unauthorized Viewing of County Data

All terminals / computer screens must be protected from the view of unauthorized persons. All confidential member information, electronic or printed, shall be protected at all times.

Passwords

The sharing of passwords or allowing unauthorized individuals access into the system is strictly prohibited. A user's password is his/her electronic signature that is not to be shared or made available to anyone. Programs must ensure that the County's Policy and Procedures regarding security and confidentiality as stated in the Summary of Policies must be complied with at all times. Failure to comply with these policies and procedures can result in the temporary or permanent denial of access privileges and/or disciplinary action.

SmartCare passwords:

- Minimum of eight (8) characters
- At least one (1) numerical digit
- At least one (1) lower case letter
- At least one (1) upper case letter
- At least one (1) special character (* - #)
- Must be reset every ninety (90) days. Users will be prompted at the end of each ninety (90) day period.

Multi-Factor Authentication

To ensure the best possible security of member data, SmartCare will utilize multi-factor authentication (MFA) to all contracted users. 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.

- MFA will be required every twenty-four (24) hours to access SmartCare

- Users will need to enter security questions - answers are not case sensitive and autofill will populate incorrect answers for security questions

- The change will not impact users who login via Akamai with a San Diego County email address.

- See the following link for more information: MFA Re-Launch Information Staff Termination Process

User Termination from SmartCare

The MIS Unit is responsible for deactivating SmartCare staff accounts.

- **Routine User Termination –** In most cases, staff employment is terminated in a routine manner in which the employee gives an advanced notice. Within one business day of employee termination notice, the program manager shall email to BHSEHRAccessRequest.HHSA@sdcounty.ca.gov and BHSCredentialing@optum.com a completed ARF with the termination date *(will be a future date).* The MIS Unit will enter the staff expiration date in SmartCare which will inactivate the staff account at the time of termination.

- **Quick User Termination –** In some situations, a staff person's employment may be terminated immediately. In this case, the program manager must immediately email the MIS Unit to request the staff account be inactivated immediately. Within one business day, the program manager shall email a completed ARF to the MIS Unit to BHSEHRAccessRequest.HHSA@sdcounty.ca.gov and BHSCredentialing@optum.com.

Legacy System: CCBH

As of 01/01/2026, the legacy solution, Cerner Community Behavioral Health (CCBH) will be retired Access will no longer be available to this system.

All member demographic information from the legacy systems (CCBH & SanWITS) has been made available in the current SmartCare solution. Pertinent member information was migrated to the new system during the transition. All historic information in the legacy CCBH system has been archived and is accessible with a chart request form through the Optum support desk (1- 800-834-3792).

AI-Assisted Documentation and Audio Processing in SmartCare

Artificial Intelligence (AI) tools integrated with SmartCare may be used to support clinical documentation workflows. These tools may assist with transcription, summarization, compliance guidance, or drafting of clinical documentation.

Some AI-assisted documentation tools may process audio from clinical encounters to generate transcripts or documentation summaries. Audio processing may occur through secure systems integrated with SmartCare and approved by the County.

AI-assisted documentation tools are intended to support Direct Service Provider documentation and workflow efficiency. These tools do not replace clinical judgment or the responsibility of the Direct Service Provider to ensure accuracy and compliance with Medi-Cal and County documentation requirements. For purposes of this guidance, **Eleos** is the AI-assisted documentation tool currently approved by BHS and integrated with SmartCare.

Use of Eleos is governed by Behavioral Health Services (BHS) policies and County requirements related to artificial intelligence, privacy, and data security. Use of Eleos shall comply with County of San Diego Board Policy A-140 (Artificial Intelligence) and any applicable contractual requirements. Eleos-generated documentation is considered draft content and must be reviewed, edited as necessary, and approved by the Direct Service Provider before it is finalized in the medical record.

Direct Service Providers remain responsible for ensuring that documentation:

- Accurately reflects services delivered
- Supports medical necessity when applicable
- Complies with Medi-Cal documentation requirements

Eleos use is intended to support documentation workflows but may not always be available. Direct Service Providers remain responsible for completing timely documentation in SmartCare in accordance with Medi-Cal and County documentation requirements when Eleos is unavailable. Eleos may not be used to generate documentation for services that were not provided or otherwise misrepresent clinical services rendered.

Direct Service Provider Responsibilities

When Eleos is used:

a. The Direct Service Provider shall review all Eleos documentation.

b. The Direct Service Provider shall edit or correct documentation as necessary to ensure the content accurately reflects the service delivered.

c. The Direct Service Provider shall approve the final documentation before submitting the note in SmartCare.

d. The Direct Service Provider remains the author of the finalized clinical documentation.

Audio Processing During Clinical Encounters

a. When Eleos is used during clinical encounters:

   i. Direct Service Providers should inform the member that AI-assisted technology is being used to support documentation during the encounter.

   ii. Consent must be obtained and documented in the clinical record prior to the use of Eleos.

   iii. Direct Service Providers should confirm consent with the member at the beginning of each session for Eleos to be used. This verbal consent at the beginning of each session shall be documented.

   iv. If a member withdraws consent, Eleos shall no longer be used.

   v. For group services, Eleos may only be used if all participating members have provided consent. If any participant declines or withdraws consent, Eleos shall not be used for that group session.

   vi. The member may ask questions about the technology used during documentation.

   vii. Audio processing may occur for the purpose of generating a transcript or documentation summary.

   viii. Audio processed by Eleos is handled in accordance with County privacy, security, and data governance policies.

   ix. Direct Service Providers must ensure that member information is processed only through County-approved systems integrated with SmartCare.

   x. Audio retention and deletion practices are governed by the approved system configuration and applicable County requirements.

xi. Direct Service Providers shall not use external or non-approved recording or transcription tools to document clinical encounters. This includes publicly available, consumer-facing, or non-secure Artificial Intelligence tools or platforms.

Use of AI Documentation Suggestions

a. Eleos may generate documentation suggestions, prompts, or compliance alerts. Direct Service Providers may:

b. Accept suggested documentation.

i. Modify suggested documentation.

ii. Override suggested documentation when the suggestion does not accurately reflect the service delivered.

iii. Direct Service Providers must exercise professional judgment when determining whether Eleos-generated content should be included in the clinical record.

iv. Direct Service Providers must apply clinical judgment and/or consult with a clinical supervisor before making decisions that impact the type or amount of care provided if and/or when Eleos content is used to support clinical decision-making.

v. Eleos-generated content may not replace required clinical supervision, assessment, or clinical decision making.

Documentation Requirements

a. Documentation created with Eleos must:

i. Accurately reflect services delivered during the encounter.

ii. Comply with Medi-Cal and County documentation requirements.

iii. Support medical necessity where applicable.

b. Eleos-generated documentation must be reviewed and edited as needed before it is finalized in the medical record

Privacy and Confidentiality

a. Use of Eleos must comply with all applicable privacy and confidentiality requirements, including:

    i. HIPAA

    ii. 42 CFR Part 2

b. Member information may only be processed through County-approved AI systems integrated with SmartCare, unless otherwise authorized by BHS.

c. Direct Service Providers shall not enter member information into external or non-approved AI tools without prior written approval from BHS. This includes generative AI platforms, transcription services, publicly available AI platforms, or other AI-enabled tools that are not approved by the County.

d. Direct Service Providers seeking to use AI tools that are not integrated with SmartCare must submit a request to BHS at QIMatters.HHSA@sdcounty.ca.gov prior to implementation. BHS will review the request and, as applicable, coordinate with DHCS to determine whether the proposed AI tool is permissible. Direct Service Providers must not use such AI tools until approval is confirmed by BHS.

Training

a. Direct Service Providers authorized to use Eleos must complete required training prior to using the system. Training includes:

    i. Appropriate use of Eleos.

    ii. Review and editing of Eleos-generated documentation.

    iii. Medi-Cal documentation expectations.

    iv. Privacy and confidentiality protections.

    v. Member notification and consent requirements related to Eleos.

    vi. Any County-required AI-related training.

Contracted Organization (Legal Entity) AI Policy Requirement

a. Contracted Organizations must develop, implement, and maintain organizational policies and procedures (P&P) governing the use of Eleos that aligns with County Board Policy A-140, the BHS AI Policy, this guidance, applicable laws and regulations, and other applicable BHS requirements.

b. Prior to receiving access to Eleos, Contracted Organizations must provide confirmation, in a form specified by BHS, that the required organizational AI policies and procedures have been developed and implemented and will be made available to BHS upon request. Confirmation may be required from Legal Entity leadership, Program Managers, or other authorized organizational representatives.

c. At a minimum, the Organization's Eleos-related P&P should address:

    i. **Governance and Oversight** Identification of responsible roles for AI use within the organization and processes to ensure alignment with County Board Policy A-140, the OPOH/SUDPOH, and other applicable County and BHS requirements. P&P should address internal oversight, risk mitigation, staff accountability, and processes for responding to concerns related to AI use.

    ii. **Human Oversight and Accountability.** Requirements that Eleos-generated outputs are reviewed, edited as necessary, and approved by the direct service provider, and that the direct service provider remains responsible for the accuracy and completeness of all finalized documentation. Eleos may not replace clinical judgment or required supervision.

    iii. **Privacy and Data Protection.** Safeguards to ensure compliance with applicable privacy and confidentiality laws (e.g., HIPAA, 42 CFR Part 2), as well as County and BHS data protection requirements, including use of only County-approved or otherwise authorized systems.

    iv. **Member Communication and Education.** P&P should address how members will be informed about Eleos, including use of approved educational materials, responses to common member questions, and communication regarding member rights and available alternatives.

v. **Member Notification and Consent.** Processes for informing members when Eleos is used in care, including how notification and consent are obtained and documented consistent with County and BHS requirements. P&P should address:

- notification that AI-assisted technology is being used;
- documentation of consent consistent with County requirements;
- member right to decline participation;
- obtaining and documenting consent prior to the use of AI-assisted documentation tools;
- ongoing notification of AI-assisted technology prior to every use;
- reminding members of their right to withdraw consent at any time;
- procedures for continuing services when a member declines use of AI-assisted tools.

vi. **Appropriate and Prohibited Uses.** Clear expectations regarding permissible uses of Eleos, including the prohibition of use to generate documentation for services not provided or to otherwise misrepresent services. P&P should also prohibit the use of non-approved AI tools, unauthorized recording or transcription applications, and the entry of member information into systems not approved by the County or BHS.

vii. **Staff Training.** Requirements for staff training on appropriate AI use, including responsibilities for review, editing, and compliance with documentation, privacy, and consent-related expectations, as well as completion of all vendor-related training (e.g., Eleos-provided or CalMHSA-provided), County-required AI-related training, and any other training required for the authorized use of AI-assisted tools. Training should address:

- appropriate use of AI-assisted tools;
- review and editing of AI-generated content;

- privacy and confidentiality requirements;
- member notification and consent requirements;
- documentation standards and accountability.

viii. **Monitoring and Compliance.** Processes for monitoring AI use within the organization to support documentation quality, compliance, staff training, and adherence to County and BHS requirements. Monitoring activities should support quality improvement, compliance oversight, staff training, workflow optimization, risk mitigation, and adherence to County and BHS requirements and should not be used for routine employee surveillance.

ix. **Documentation Standards and Accountability.** Requirements that Eleos-generated content be treated as draft content until reviewed, edited as necessary, and finalized by the direct service provider. P&P should clearly state that Eleos does not replace clinical judgment and that staff remain responsible for the accuracy, completeness, and compliance of finalized documentation.

x. **Approved Technology Use.** P&P should prohibit the use of non-approved AI-assisted documentation tools, recording applications, or transcription services for County-funded services unless expressly authorized by BHS.

d. Contracted Organizations must maintain documentation of their AI policy and make it available to BHS upon request.

e. Contracted Organizations must maintain documentation of their AI policy and make it available to BHS upon request.

Quality Oversight

a. BHS may review documentation created using Eleos as part of routine quality assurance and compliance monitoring activities.

b. Monitoring may include:

i. Documentation audits

ii. Review of documentation quality trends
iii. Analysis of system-generated compliance alerts and related documentation trends

iv. Review of findings from DHCS audits or External Quality Review (EQR).

c. Monitoring activities are intended to support quality improvement, compliance oversight, training, workflow optimization, and program evaluation and are not intended for routine employee surveillance.

d. Direct Service Providers may receive feedback or additional training based on monitoring findings.

e. The County reserves the right to review, monitor, and require modification or discontinuation of Eleos use if compliance, privacy, or documentation risks are identified.

Resource Guide

Need	Resource	Contact Information
System Issues (i.e. glitches, functionality issues, pop up errors)	CalMHSA Live Chat	www. 2023.calmhsa.org After normal business hours the only support available is for system outages: (916) 214-8348
SmartCare ARF submission and any access related issues or questions	Email	BHS_EHRAccessRequest.HHSA@sdcounty.ca.gov
Support questions that cannot be addressed by the CalMHSA Support Desk	Email	BHS_EHRSupport.HHSA@sdcounty.ca.gov
Questions related to documentation, guidelines or policy	Email	QIMatters.HHSA@sdcounty.ca.gov
Escalation of CalMHSA help desk issues resolved prematurely or not resolved entirely	Email	BHS_EHRSupport.HHSA@sdcounty.ca.gov
Optum Support Desk	Phone Email	1-800-834-3792 sdhelpdesk@optum.com