J. MANAGEMENT INFORMATION SYSTEMS (MIS)

Technology Requirements

Providers shall maintain technology that facilitates the collection, maintenance, and reporting of data necessary to comply with the County of San Diego and California Department of Health Care Services data requirements. Provider's computer-based data collection, maintenance, and reporting systems shall comply with current County and State standards. For more information regarding SmartCare technology requirements, go to HardwareSoftwareRequirements_Mar2024.pdf at the Optum website.

Providers shall have at least one computer with internet access. Treatment data shall be entered electronically into SmartCare; DATAR data shall be entered into DATARWeb; other required reports and forms shall be submitted electronically to the MIS Support Desk.

All providers shall be capable of transmitting and receiving information through email. Communications to the provider regarding compliance issues, system related issues, and requirements are sent through email from the MIS unit. Providers need to maintain an email address and shall notify the COR or COR's designee and the MIS unit of any change in email addresses within two business days of the effective date of the change. The MIS unit can be notified of email updates by sending an email to **BHS_EHRAccessRequest.HHSA@sdcounty.ca.gov**.

All electronic provider files containing DHCS PHI or PI and stored on removable media or portable devices shall be encrypted with a FIPS 140-2 certified algorithm.

County TLS Email Encryption

The county has Transport Layer Security (TLS) available for sending encrypted email through a secured connection. This means when a TLS connection is established with a vetted County business partner, all email communication sent between the County and the business partner will be automatically encrypted in transit over the internet through the secured connection. Contact the County BHS COR or COR's designee for more information about TLS and how to initiate the process for your agency.

Electronic Health Records

DHCS requires that programs utilizing an Electronic Health Record (EHR) have the following available to DHCS staff during an audit, licensing, or certification review:

- Physical access to the EHR system
- Adequate computer access to the EHR needed for the audit or review
- Access to printers and capability to print necessary documents
- Technical assistance as requested
- Scanned documents, if needed, that are readable and complete

Additionally, DHCS requires programs using an EHR to obtain a signed "Electronic Signature Agreement" from all users who will be signing financial, program or medical records with an electronic signature. This agreement should include, among other things, that the signer has an obligation to protect their electronic signature (id/password), to keep their sign-in information secret and to not share the information, and to notify appropriate program staff if it is stolen, lost, compromised, unaccounted for, or destroyed.

Programs should contact their County BHS COR to notify them if they are planning to implement an EHR

as BHS is required to certify that the system used meets DHCS standards. For more information, see ADP Bulletin 10-01 and its exhibits. Programs shall have all SUDURM forms created for the EHR approved by SUDQA. Programs shall have internal policies and procedures in place for EHR use, to include how to handle client documentation when a system outage occurs or the EHR is unavailable.

SmartCare

A semi-statewide electronic health record (EHR) offered through California Mental Health Authority (CalMHSA) has replaced SanWITS as the EHR for SUD system of care (SOC). SmartCare was designed specifically for California's behavioral health systems and meets all state reporting and billing requirements for CalAIM payment reform. It meets 42 CFR Part 2 privacy requirements and includes a robust consent management tool. SmartCare provides more efficient and streamlined workflows that satisfy CalAIM requirements.

In SmartCare, contracted treatment providers are set up by programs within a secure treatment site Clinical Data Access Group (CDAG) to ensure users have access to only the information they need to fulfill their job functions.

While the County is working toward interoperability with other systems, providers with their own EHR will need processes to accommodate dual entry of specific client data, state reporting, and billing.

Trainings

- The CalMHSA's LMS trainings found here https://moodle.calmhsalearns.org/login/index.php are mandatory for all SmartCare users prior to receiving access to SmartCare.
- SmartCare users will also be able to schedule supplemental trainings online as applicable to their job functions.
- The SmartCare ARF can be found on regpack and should be submitted to BHS_EHRAccessRequest.HHSA@sdcounty.ca.gov
  SmartCare Resources:
- For any system-related issues, please reach out to CalMHSA. SmartCare Helpdesk Support Information
- For trouble accessing the system, please send your email to BHS_EHRAccessRequest.HHSA@sdcounty.ca.gov

- For questions related to documentation, guidelines, or policy, please send your email to QIMatters.HHSA@sdcounty.ca.gov.
- If you would like to request a program or system change, or for deletions, please send your email to BHS_EHRSupport.HHSA@sdcounty.ca.gov

Client Requests for Amendment and Client Requests for Accounting of Disclosure

- When a Program receives a request to amend electronic health records and believes amendments need to be made the program should contact the SDCBHSM IS team at BHS_EHRSupport.HHSA@sdcounty.ca.gov and the Agency Compliance Office at 619-338-2808 or privacyofficer.hhsa@sdcounty.ca.gov, to provide Program assistance as needed.

When a program receives a request to amend records within their internal electronic health records, the program should work with their Compliance Officer and follow internal policies and procedures in

alignment with related regulations. Client Requests for Accounting of Disclosure.

When a Program receives a request for an accounting of disclosures of electronic health records, the program should follow their internal policy and procedures established for release of information (ROI). The legacy system - SanWITS will still be used for all services and state reporting dated prior to September 1, 2024, as well as any corrections for billing or state reporting as needed.