F. COMPLIANCE & CONFIDENTIALITY

The County of San Diego Health and Human Services Agency (HHSA) shall adhere to all laws, rules, and regulations, especially those related to fraud, waste, abuse, and confidentiality.

Compliance

Record Retention
Per WIC 14124.1, records are required to be kept and maintained under this section shall be retained:

- by the provider for a period of 10 years from the final date of the contract period between the plan and the provider,
- from the date of completion of any audit,
- or from the date the service was rendered, whichever is later, in accordance with Section 438.3(u) of Title 42 of the Code of Federal Regulations

Documentation Requirements
To promote consistency and standardization of County of San Diego required record documentation, a Uniform Record Manual (SUDURM) was implemented July 1, 2014. The SUDURM contains all required forms to ensure documentation compliance to Federal, State, and County laws and regulations under Title 9, Chapter 11, and 42 CFR. SUD providers are required to complete County-required protocols (including documentation standards and timelines) for assessment, treatment plans/problem lists, level of care determination, progress notes, and other documentation requirements as specified within the SUDURM and SUDPOH. Within the SUDURM, documentation forms are filed in specific order starting with Section 1: Intake/Financial and ending with Section 8: Drug Test Results/Reports. Individual programs are responsible for ensuring their providers utilize the required forms within the SUDURM as appropriate. SUDURM forms are located on the Optum San Diego website. Directions regarding access to this website can be found in the Appendix F.1 - Optum Website Tip Sheet.

False Claims Act
All HHSA employees, contractors, and subcontractors, are required to report any suspected inappropriate activity. Suspected inappropriate activities include but are not limited to, acts, omissions or procedures that may be in violation of health care laws, regulations, or HHSA procedures. The following are examples of health care fraud:

- Billing for services not rendered or goods not provided
  - Falsifying certificates of medical necessity and billing for services not medically necessary
  - Billing separately for services that should be a single service
  - Falsifying treatment plans or medical records to maximize payment
  - Failing to report overpayments or credit balances
  - Duplicate billing
  - Unlawfully giving health care providers such as physicians' inducements in exchange for referral services.

If any County or Contracted program needs training on the False Claims Act, reach out to the BAC at 619-338-2808 or email Compliance.HHSA@sdcounty.ca.gov.
In addition, any potential fraud, waste, or abuse shall be reported directly to DHCS' State Medicaid Fraud Control Unit. Reporting can be done by phone, online form, email or by mail.

- 1-800-822-6222
- fraud@dhcs.ca.gov
- Medi-Cal Fraud Complaint – Intake Unit Audits and Investigations

- P.O. Box 997413; MS 2500 Sacramento, CA 95899-7413

All reporting shall include contacting your program COR immediately, as well as the BHS QA team at QIMatters.HHSA@sdcounty.ca.gov to report any of these same concerns, or suspected incidents of fraud, waste, and/or abuse.

Program Integrity/Service Verification
San Diego County Behavioral Health Services (SDCBHS) established Program Integrity (PI) procedures to prevent fraud, waste, and abuse in the delivery, claiming and reimbursement of behavioral health services. County and Contracted Programs shall develop a process of verifying that paid claims were provided to members and that services were medically necessary. County and Contracted Programs are expected to conduct regular PI activities and maintain records for audit purposes. Questions regarding PI can be directed to QI Matters email at QIMatters.HHSA@sdcounty.ca.gov.

PI activities will be monitored by QA at a minimum annually during site and medical record review. QA tracks and monitors results of medical record reviews and may require a program to develop a Quality Improvement Plan (QIP) to address specific documentation concerns.

Mandated Reporting
All treatment providers shall adhere to mandated reporter requirements regarding child abuse and neglect, elder abuse and neglect, and homicide or homicidal ideations (California Welfare and Institutions Code section 15630 and California Penal Code section 11164). Mandated reporting as required by law is not to be considered unauthorized release of confidential information. Permissive exceptions to confidentiality may include:

- Danger to self
- Danger to others
- Another's property
- When such disclosure is necessary to prevent the threatened danger (Tarasoff Notification)

For further information regarding legal and ethical reporting mandates, contact your agency's attorney, the State licensing board, or your professional association.

Confidentiality

Client and community trust is fundamental to the provision of quality mental health services and abiding by confidentiality rules is a basic tenet of that trust. Thus, County and Contracted workforce members shall follow all applicable state and federal laws regarding the privacy and security of information.

SUD Quality Assurance (QA) Responsibilities & Confidentiality
In order to ensure compliance with confidentiality procedures and protocols, the SUD QA enforces the following procedures:

- Every member of the workforce is informed about confidentiality policies as well as applicable state and federal laws regarding anonymity and the confidentiality of clinical information.
- As a condition of employment, each member of the workforce signs a confidentiality agreement promising to comply with all confidentiality protocols. This statement must include a minimum General Use, Security and Privacy safeguards, Unacceptable Use, and Enforcement Policies.
    - The statement must be signed by the workforce member prior to access to protected health information (PHI). PHI stands for Protected Health Information. It is any health data that is individually identifiable and relates to the past, present or future physical or mental health of an individual. PHI can be in many forms, including written records, electronic

records, images and information shared verbally. While not an exhaustive list, the following are considered individually identifiable data: patient names, Social Security numbers, phone numbers, email addresses, dates related to health or identity, biometric identifiers, electronic health records, and images that could identify the subject.

- The statement must be renewed annually.

Any client treatment records gathered during the course of provision of services, provider site and record reviews, or as necessary are protected through strictly limited access. Program staff have access to case data or files only as necessary to do their jobs.

Providers within the County of San Diego SUD system of care demonstrate ongoing commitment and compliance to the protection of client personal and health information as defined in 42 CFR Part 2, Health Insurance Portability and Accountability Act of 1996 (HIPAA), the State/County agreement, and other Federal, State regulations/laws through:

1. Established written policies and procedure to address workforce members' code of conduct to include protection of client confidentiality while providing services within the SUD system of care. ("Workforce members" includes, but is not limited to, all employee types, including per diem/contracted/temporary volunteers, students/interns, subcontractors, and others with access to clients and/or client data).

2. Verifiable program orientation and/or trainings/staff meetings, with focus on current/updated client confidentiality/disclosure information and applicable Federal and State laws governing such.

3. All workforce members, working within the SUD system of care, are required to sign an agreement to comply with all confidentiality protocols as defined by law, regulation, and program code of conduct policy and procedure.

4. The Confidentiality Agreement must include language in which the workforce member agrees to not divulge personal information (PI), personally identifiable information (PII), and protected health information (PHI) to any unauthorized person or organization unless authorized or required by law. PI, PII and PHI definitions are found in Article 14 of the program's contract with the County.

5. Workforce members will be given access to client PHI after # 1 and # 2 are completed.

6. Workforce members will renew their Confidentiality Agreement annually as verified by signature and date on the statement and placement within their personnel record.

7. Programs will have written policies and procedure which identify potential sanctions should violations of unauthorized release of confidential client health information occur.

8. Providers will respect a client's right to revoke their consent/authorization to disclose information in part or whole. Should this occur, the SUD treatment providers must notify the involved entities of this update immediately.

All substance use disorder treatment services shall be provided in a confidential setting in compliance with 42 CFR, Part 2 requirements. If services were provided in the community, documentation must identify the location and how the provider ensured confidentiality.

Final Rule, 42 CFR Part 2

The SUD system of care is moving into a new era that encourages information sharing with the physical and mental health systems for improvement of care coordination and client health outcomes. (See Examples of Permissible Payment and Healthcare Operations Activities below.)

It is well recognized that SUD clients often have additional health conditions that complicate care and can prevent long-term achievement of recovery goals if left un/under treated.

Final Rule, 42 CFR Part 2, published February 16, 2024, effective April 16, 2024, implements new changes to the federal rules governing confidentiality and disclosures of substance use disorder patient records, known as 42 CFR Part 2 or "Part 2" to afford persons with substance use disorder, receipt of integrated and coordinated care while still protecting client confidentiality. While the new Final Rule maintains Part 2's core protections, including consent requirements, it expands the ways in which patients' protected substance use disorder information may be shared. It aligns several provisions with HIPAA regulations including allowing for a single consent for TPO, penalties, breach notification, patient notice and Safe Harbor. For more information, please reference the Final Rule 42 CFR Part 2.

Examples of Permissible Payment and Health Care Operations Activities under 42 CFR Part 2 Section 2.33(b) SAMHSA:

- Billing, claims management, collections activities, obtaining payment under a contract for reinsurance, claims filing and related health care data processing
- Clinical professional support services (e.g., quality assessment and improvement initiatives; utilization review and management services)
- Patient safety activities
- Activities pertaining to the training of student trainees and health care professionals
- Activities pertaining to the assessment of practitioner competencies
- Activities pertaining to the assessment of provider and/or health plan performance, and
- Activities pertaining to the training of non-health care professionals
- Accreditation, certification, licensing, or credentialing activities
- Underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care
- Third-party liability coverage
- Activities related to addressing fraud, waste and abuse
- Conducting or arranging for medical review, legal services, and auditing functions
- Business planning and development, such as conducting cost-management and planning related analyses related to managing and operating, including formulary development and administration, development or improvement of methods of payment or coverage policies
- Business management and general administrative activities, including management activities relating to implementation of and compliance with the requirements of this or other statutes or regulations
- Customer services, including the provision of data analyses for policy holders, plan sponsors, or other customers
- Resolution of internal grievances
- The sale, transfer, merger, consolidation, or dissolution of an organization
- Determinations of eligibility or coverage (e.g., coordination of benefit services or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims
- Risk adjusting amounts due based on enrollee health status and demographic characteristics

- Review of health care services with respect to medical necessity, insurance coverage under a health plan, appropriateness of care, or justification of charges.

SUD providers are advised to contact the legal representative within their organizations for legal interpretation and direction in regard to application of Confidentiality Law/Regulations to program specific policy and procedure. Should legal entities or programs have further questions regarding interpretation of 42 CFR Part 2 Final Rule, please see more information through the County of San Diego Health & Human Services Business Assurance & Compliance Office.

Federal Delegation of Authority to OCR: The federal HHS Secretary issued a formal Delegation of Authority for enforcement of 42CFR Part 2 to the federal Office of Civil Rights (OCR).

This is the latest step in a process initiated by the CARES Act in 2020 to align the Part 2 substance-use disorder privacy rule more closely with HIPAA. As part of those changes, the CARES Act revised the enforcement scheme so that the civil and criminal penalties applicable to HIPAA are also applicable to Part 2 violations (previously, Part 2 was purely enforceable through criminal authorities). HHS finalized the rule implementing the CARES Act changes in February of last year. That rule clarified—consistent with the CARES Act—that violations of Part 2 would be subject to the same penalties as violations of HIPAA. Now HHS has further implemented the change by delegating enforcement authority to OCR, which is the same entity that enforces HIPAA. They have also delegated Part 2 implementation and interpretation authority more broadly to OCR. The federal regulatory body enforcing Part 2 is now an agency with a specialized expertise in privacy and a broader toolkit of enforcement tools, including civil penalties in addition to criminal penalties.

It is suggested that Legal Entities review their Part 2 compliance programs and make sure they are up to date with the substantial changes that have been made by the CARES Act.

Client Confidentiality

Providers shall comply with federal client confidentiality regulations (Confidentiality of Substance Use Disorder Patient Records- 42U.S.C.290dd-2; 42CFR part 2), and all applicable Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations.

Client Answering Program Business Phones

Providers shall have trained provider staff available to answer business phone calls during hours of operation. Program shall ensure participants in DMC-ODS programs shall not answer phones on behalf of program staff. Providers shall ensure client confidentiality is maintained at all times.

Client File Storage and Transportation

Sites must keep a record of the clients/patients being treated at that location. If it is required to transport records offsite, to maintain the confidentiality of all client files and medical records, the standard protocol for storing confidential material shall be maintained until transport is possible. Client files are to be stored under double lock and key (i.e., locked cabinet in a locked room) at the program location. No client files are to be taken to staff's private residences. The program supervisor shall designate staff members who will be responsible for the transportation of client files. A staff member shall inform the program director if file transport is necessary. Client files shall be transported in a portable locked file box. When transporting identifying client data or medical records such as progress notes or forms requiring signatures, no identifying information shall be put on the documents until which time said documents are secured in the client's medical record at the primary clinic where the record is being stored. Progress notes or other individual documents transported while in the field shall not contain the full name of the client. Under no circumstances are any records to be left unattended.

Off Site Record Storage
Programs shall notify their program COR when client records are moved offsite permanently (i.e., records moved to storage).

Cloud-Based Record Storage
Cloud-based storage for client records is an option for providers. Expectations for this option include Article 14 requirements, including the DHCS SUD Agreement, in the contract with the vendor providing the service. Contracted providers are also expected to vet and monitor the vendor and services to ensure compliance. For additional information on the DHCS SUD agreements, see the County of San Diego Health & Human Services Business Assurance & Compliance Office.

Client Requests for Records
When a client (or the individual with authority of the record) requests access to or a copy of their record, all Programs shall abide by applicable privacy laws and reasonably ensure the identity of the requestor before turning over client information. Remember that client requests for records are not the same as a request for records from a third party; different rules apply. County Programs shall follow the relevant BAC policies and procedures related to record requests (HHSA L-01). Contracted Programs may, but are not required, to use the HHSA Client Record Request Form (HHSA 23-01). If a Contracted Program chooses to use the HHSA form, it must replace the HHSA logo and contact information with its own and should also review the contents of the HHSA form to ensure it meets all applicable privacy requirements. Contracted programs may also use their own form so long as it complies with all applicable rules and regulations. Contracted Programs shall also have a Client Request for Records policy to ensure these requirements are followed by workforce members.

State law, 45 CFR 164.524, regarding a client's access to health records requires the following:

- Client records may be requested by any adult client, client personal representative, minor client authorized by law to medical treatment, or attorney.
- Health care providers cannot require a client's request for health records to be submitted in writing.
- Requires health care providers to provide a copy of the records in a paper or electronic copy, in the form or format requested if the records are readily producible in that form or format.
- Requires health care providers to permit inspection of client records during business hours within five (5) working days after the receipt of the request.
- Requires health care providers to provide copies within fifteen (15) days after receiving the request.
- Requires health care provider fees to be based on specified costs for labor, supplies, postage, and preparing an explanation or summary of the client record instead of clerical costs. These costs are capped.
- Prohibits health care providers from withholding client records because of unpaid bills for health care services.
- Health care providers no longer can provide a summary in lieu of the actual record unless agreed upon by the client.
- Allows disclosure to a business associate for health care operations purposes.

Adult and minor child clients who consent or could have consented to their own treatment have a right to access their own records. Providers cannot refuse access based on the provider's judgement that access would interfere with the therapeutic relationship or cause emotional harm. A summary of the record is not an acceptable alternative to providing access to the record. Parent access, however, can be limited if the minor child client consented or could have consented to the care.

Record Requests Past 365 Days (SmartCare)

The County of San Diego BHS manages an electronic health record (EHR) for the BHP County and contracted providers (SmartCare). Contracted providers have access to a client's chart for 365 days post-discharge to respond to record requests accordingly. Once that timeframe expires, a request will need to be made via the Optum Help Desk to access documents past one year. Optum will grant access for 72 hours, closing the record again after that time.

DAYS	HOURS	CONTACT
Monday - Friday	6:00 am to 6:00 pm	1-800-834-3792

CalMHSA has the following additional instructions on the Release of Information processes:

- How to Document a Release of Information (Authorization to Disclose Confidential Information
- How to Revoke a Standard Release of Information/Authorization to Disclose Information
- How to Determine What Disclosure Authorizations (Release of Information) the Client has Signed

Notice of Privacy Practices

County and Contracted Programs must provide a HIPAA-compliant Notice of Privacy Practices (NPP) to all clients, as well as those with authority to make treatment decisions on behalf of the client. A notation is made on the Behavioral Health Assessment form when the NPP has been offered. Providers should ensure clients (and those with authority) understand the NPP and address any client questions about client privacy rights and the Program's privacy requirements.

County Programs shall use the HHSA NPP and adhere to all related policies and procedures (HHSA L-06), including the NPP Acknowledgement form (HHSA 23-06), all of which are available on the BAC website at www.cosdcompliance.org. Contracted Programs may, but are not required, to use the HHSA NPP. If a Contracted Program chooses to use the HHSA NPP, it must replace the HHSA logo and contact information with its own and should also review the contents of the HHSA NPP to ensure it meets all applicable privacy requirements. Contracted Programs shall also have an NPP policy or procedure to ensure NPP requirements are followed by workforce members.

Privacy Incidents

A privacy incident is an incident that involves the following:

- Unsecured protected information in any form (including paper and electronic); or
- Any suspected incident, intrusion, or unauthorized access, use, or disclosures of protected information; or
- Any potential loss or theft of protected information.

Common Privacy Incidents may include, but are not limited to:

- Sending emails with client information to the wrong person
- Sending unencrypted email with client information outside of your legal entity
- Giving Client A's paperwork to Client B (even if you immediately get it back)
- Lost or stolen charts, paperwork, laptops, or phones
- Unlawful or unauthorized access to client information (peeking issues)

If any Program believes that a privacy incident has occurred, they must complete the applicable HHSA privacy incident reporting. For Contracted Programs, this is outlined in Article 14 of your County contract. For County programs, follow BAC policies and procedure (L-24). All programs shall immediately notify the BAC Privacy Officer and COR via email. Programs shall submit an initial Privacy Incident Report (PIR) online within one (1) business day. To access the landing page and link to the PIR web-form, these documents can be found at www.cosdcompliance.org.

Contracted Programs must additionally ensure compliance with HIPAA breach requirements, such as risk analysis and federal reporting and inform the BAC of any applicable requirements.

Privacy Incident Reporting (PIR) for Staff and Management

- Staff becomes aware of a suspected or actual privacy incident.
- Staff notifies Program Manager immediately.
- Program Manager notifies County COR and Privacy Officer immediately upon knowledge of incident.
- Program Manager completes the online Privacy Incident Report within one business day.
- Continue investigation and provide daily updates to the Privacy Officer.
- Updates to the online Privacy Incident Report should be made through the same online reporting portal within 7 business days.
- Complete any other actions as directed by the Privacy Officer.

San Diego County contracted providers should work directly with their agency's legal counsel to determine external reporting and regulatory notification requirements. See Appendix F.2 for more information. Additional compliance and privacy resources are available at: https://www.sandiegocounty.gov/hhsa/programs/sd/compliance_office/