D. Compliance and 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.

Reporting Fraud, Waste and/or Abuse

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.

Medi-Cal Fraud Complaint – Intake Unit Audits and Investigations
1-800-822-6222 | Fraud@dhcs.ca.gov
P.O. Box 997413 MS 2500 Sacramento, CA 95899-7413

Any indication that any one of these activities is occurring including suspected fraud, waste and/or abuse, should be reported immediately to your program COR, as well as the BHS QA team at QIMatters.HHSA@sdcounty.ca.gov. If there is a need to remain anonymous, then providers may contact Business Assurance & Compliance (BAC) at ((619) 237-8571 or email Compliance.HHSA@sdcounty.ca.gov

False Claims Act

The Federal False Claims Act (FCA) helps the government combat fraud in federal programs, purchases, and contracts and applies to fraud involving state, city, county or other local government funds. All workforce members shall report any suspected inappropriate activity related to these Acts, which include acts, omissions or procedures that may violate the law or HHSA procedures. Some examples include billing for services not rendered or not medically necessary, billing separately for services that should be a single service, falsifying records and/or duplicate billing.

The FCA encourages voluntary disclosure of fraudulent activities by rewarding individuals who report fraud and allowing courts to waive penalties for organizations that voluntarily disclose false claims. Programs and legal entities may not have any rule that prevents workforce members from reporting, nor may programs or legal entities retaliate against a workforce member because of his or her involvement in a false claims action. County and County Contracted Programs are required to promptly report circumstances that may affect the members' eligibility to the California Department of Health Care Services (DHCS). They are also required to conduct an internal investigation to determine the validity of the issue/complaint as well as develop and implement corrective action, if needed.

If any County or Contracted program needs training on the False Claims Act, reach out to the BAC at 619-237-8571 or email Compliance.HHSA@sdcounty.ca.gov

Compliance for County and Contracted Programs

As part of this commitment, all County Behavioral Health Services workforce members shall be familiar with and adhere to Business Assurance & Compliance (BAC) policies and procedures. County Behavioral Health Programs shall have processes that ensure adherence to the HHSA Code of Conduct. All BAC policies and procedures, including the Code of Conduct, may be found on the BAC website. Contracted providers with the BHP are obligated to have an internal compliance program commensurate with the size and scope of their agency. Further, contractors with more than $250,000 (annually) in agreements with the County must have a Compliance Program that meets the Federal Sentencing Guidelines (Sections 8 B2.1 & 42 CFR 438.608(b) 1 –7) including the seven elements of an effective compliance program, listed below:

1. Development of a Code of Conduct and Compliance Standards.

2. Assignment of a Compliance Officer who oversees and monitors implementation of the compliance program.

3. Design of a Communication Plan, including a Compliance Hotline, which allows workforce members to raise complaints and concerns about compliance issues without fear of retribution.

4. Creation and implementation of Training and Education for workforce members regarding compliance requirements, reporting, and procedures.

5. Development and monitoring of Auditing Systems to detect and prevent compliance issues

6. Creation of Discipline Processes to enforce the program.

7. Development of Response and Prevention mechanisms to respond to, investigate, and implement corrective action regarding compliance issues.

Please note: Contracted programs may use their own forms so long as they comply with all applicable rules and regulations. If a Contracted Program chooses to use a County 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.

Compliance Standards

All County and Contracted Programs, regardless of size and scope, shall have processes in place to ensure at the least the following standards:

- All new employees shall receive a thorough employee orientation about compliance requirements prior to employment.
- Staff shall have proper credentials, experience, and expertise to provide member services.
- Staff shall document member encounters in accordance with funding source requirements and HHSA policies and procedures.
- Staff shall bill member services accurately, timely, and in compliance with all applicable regulations and HHSA policies and procedures.
- Staff shall promptly elevate concerns regarding possible deficiencies or errors in the quality of care, member services, or member billing.
- Staff shall act promptly to correct problems if errors in claims or billings are discovered.

Documentation Standards

Please note that it is the responsibility of the program to have staff provide services within their scope of practice. This includes co-signing of documentation as appropriate.

Reference: CalMHSA Clinical Documentation Guide- Appendix III Scope of Practice Matrix- pg. 40

Assessment Standards

To ensure that members receive the right service, at the right time, and in the right place, providers shall use their clinical expertise to complete initial assessments and subsequent assessments as expeditiously as possible, in accordance with each member's clinical needs and generally accepted standards of practice. Assessments shall be updated **as clinically appropriate,** such as when the member's condition changes.

Care Plan Standards

DHCS no longer requires prospectively completed, standalone care plans for Medi-Cal Specialty Mental Health Services. The intent of this change is to affirm that care planning is an ongoing interactive component of service delivery rather than a one-time event.

Required care plan elements may be notated within the assessment record, problem list, or service notes, or the provider may use a dedicated care plan template within the Electronic Health Record. The provider shall be able to produce and communicate content of the care plan to other providers, the member, and Medi-Cal behavioral health delivery systems, in accordance with applicable state and federal privacy laws if requested.

Federal or state laws continue to require the following services to have care plans and/or specific care planning activities in place. All required elements of the Care Plan must be addressed as indicated in Enclosure 1a of BHIN 23-068: TCM, ICC, Peer Support Services, TBS, STRTPs, Crisis Houses FSPs and Medicare recipients.

For more information on specific requirements please refer to the *Care Plan Explanation Sheet* on the Optum Website> *UCRM* tab.

Problem List Standards

All member receiving services after July 1, 2022, are required to have a Problem List documented within the EHR. The problem list is a list of symptoms, conditions, diagnoses, and/or risk factors identified through assessment, psychiatric diagnostic evaluation, crisis encounters, or other types of service encounters. Updates to the Problem List are to be completed on an on-going basis within the EHR on the "*Client Clinical Problem Details*" page as well as service notes to reflect the current presentation of the member, with problems being added or removed when there is a relevant change to the member's condition.

Service Note Standards

Providers shall create service notes for the provision of all services. Each service note shall provide sufficient detail to support the service code selected for the service type as indicated by the service code description. Notes are to be completed and signed within three (3) business days of providing a service, with the exception of notes for crisis services, which shall be completed within twenty-four (24) hours. Please be advised certain service lines have requirements which remain in effect due to applicable federal regulations or guidance, regulations which supersede these indicated timelines above. In these cases, regulations must be followed as indicated by DHCS.

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 ten (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

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.

Confidentiality for County and Contracted Programs

Member and community trust is fundamental to the provision of quality mental health services. Abiding by confidentiality rules is a basic tenet of that trust. County and Contracted workforce members shall follow all applicable state and federal laws regarding the privacy and security of information. Programs are responsible for ensuring compliance with the latest requirements within the State Agreement, which can be found at the Optum website > *Manuals* tab. If any County or Contracted provider has questions about privacy or security requirements, reach out to the BAC at 619-237-8571 or Compliance.HHSA@SDCounty.ca.gov.

To ensure compliance with applicable privacy laws as well as the State Agreement, the BHP has the following requirements for County and Contracted Programs. As of 2018, requirements include that all workforce members shall:

- Be trained in privacy and security of member data and shall sign a certification indicating the workforce member's name and date on which the training was completed. The certifications shall be kept at least six (6) years. Training must be provided within a reasonable period upon hire and at least annually thereafter. If any County or Contracted program needs assistance with privacy and security training, reach out to the BAC at 619-237-8571 or privacyofficer.hhsa@sdcounty.ca.gov.

- Sign a confidentiality statement prior to having access to member information. The signed statement must be maintained for at least six years. The statement must adhere to State Agreement requirements, currently including, at a minimum: General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies sections.

- Only access member records as necessary to perform their jobs.

- Staff shall act in accordance with good judgment, clinical and ethical standards and applicable privacy laws to ensure that all written and verbal communication regarding each member's treatment and clinical history is kept confidential.

Notice of Privacy Practices

County and Contracted Programs must provide a HIPAA-compliant *Notice of Privacy Practices (NPP)* to all members, as well as those with authority to make treatment decisions on behalf of the member. A member acknowledgement of the NPP is maintained in the EHR and/or the hybrid chart. Providers should ensure members (and those with authority) understand the NPP and address any member questions about member privacy rights and the Program's privacy requirements.

For County programs, a definition of Authority may be found at *BAC Policy and Procedure HHSA L-27*. County Programs shall use the HHSA NPP and adhere to all related policies and procedures (HHSA L-06), including *the NPP Acknowledgement form* (Client Rights and Notice of Privacy Practices). All forms are available on the BAC website. Contracted Programs may, but are not required, to use, the HHSA NPP located on the Optum Website> *Beneficiary* tab. If a Contracted Program chooses to use the HHSA NPP, it must replace the HHSA logo and contact information with its own and should review the contents of the HHSA NPP to ensure it meets all applicable privacy requirements. Contracted Programs shall have an NPP policy or procedure to ensure NPP requirements are followed by workforce members.

Privacy Incidents

A *privacy incident* (for definition, County programs may see *BAC Policy L-30*. Contracted Programs may review their Article 14) is an incident that involves the following:

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

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

- Sending emails with member information to the wrong person
- Sending unencrypted email with member information outside of your legal entity
- Giving Member A's paperwork to Member B

- Lost or stolen charts, paperwork, laptops, or phones
- Unlawful or unauthorized access to member information

Privacy Incident Reporting (PIR) Process

If any Program believes a privacy incident has occurred, they must complete the online HHSA Privacy Incident Report . For Contracted Programs, this is outlined in Article 14 of your County contract. For County programs, follow BAC policies and procedure (L-24). Contracted Programs must additionally ensure compliance with HIPAA breach requirements, such as risk analysis and federal reporting and inform BAC of any applicable requirements. Contracted providers should work directly with their agency's legal counsel to determine external reporting and regulatory notification requirements. Additional compliance and privacy resources are available at the HHSA BAC website.

Mandated Reporting

All County and Contracted workforce members shall comply with the *Child Abuse Reporting Law* (California Penal Code section 11164) and *Adult Abuse Reporting Law* (California Welfare and Institutions Code section 15630). For further information regarding legal and ethical reporting mandates, contact your agency's attorney, State licensing board, or your professional association.

Uses and Disclosures of Records

When a third-party requests member information, the program should ensure compliance with applicable privacy laws and relevant BAC policies and procedures (HHSA L-25 and HHSA L-09). Programs shall reasonably ensure the authorization is valid and verify the identity of the requestor before providing member information. County Programs shall also use the HHSA-approved authorization form (HHSA 23-09) when soliciting member records from a third party. Contracted Programs may, but are not required to, use the HHSA Authorization form located on the Optum Website > *UCRM* tab. Contracted Programs shall have an authorization policy and a Uses and Disclosures policy to ensure these requirements are followed by workforce members.

Member Requests for Records

When a member (or individual with authority of record), or a third-party request access to their record, all programs shall comply with applicable privacy laws. The Privacy Rule requires a covered entity to take reasonable steps to verify the identity of an individual making a request for access. (45 CFR 164.514(h).)

Please note that member requests for records are not the same as a request for records from a third party. 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). This form and information regarding privacy policies and procedures are located on the HHSA BAC Website- Forms. County and Contracted providers may charge a reasonable fee for labor associated with copying, supplies, postage, or preparation of summary as agreed to by the member.

Summary of PHI

The covered entity also may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided in addition to that PHI, so long as the individual in advance: a. Chooses to receive the summary or explanation (including in the electronic or paper form being offered by the covered entity); and b. Agrees to any fees that may be charged by the covered entity for the summary or explanation (45 CFR 164.524(c)(2)(iii)).

Timelines to Access Per state law, a covered entity must provide access to the PHI requested or in part, no later than five (5) business days from receiving the individual's request and copies within fifteen (15) business days after receiving the request (45 CFR 164.524(b)(2).

Contracted Providers have access to a member's medical record for three hundred and sixty five (365) days post-discharge. Once that timeframe expires, a request will need to be made via MIS to access the client's medical record. MIS will grant access for seventy-two (72) hours, closing the record again after that time.

Denial of Member Access to Records

County or Contracted providers may deny a member's request for records if a licensed healthcare professional has determined that the access requested is reasonably likely to endanger the life or physical safety of the member or another person. The member must be given the right to have such denials reviewed by a licensed health care professional designated by the BHP to act as the reviewing official and who did not participate in the original denial. The covered entity must provide a denial in writing to the individual no later than within thirty (30) calendar days of the request.

Member Requests for Amendment

When a program receives a request to amend SmartCare records and or when a program receives a request for an accounting of disclosures of SmartCare records, the program should contact the SDCBHS MIS team and, if necessary BAC at 619-237-8571 or privacyofficer.hhsa@sdcounty.ca.gov. 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.

Handling/Transporting Medical Record Documents

To maintain the confidentiality and security of member records, all programs will securely store and transport medical records, including laptops, phones, and tablets, which may contain member identifying information in accordance with applicable laws and the State Agreement:

- Member records must be maintained at a site that complies with Article 14 requirements, including the current State Agreement.
- County workforce members may, as needed, transport member records and/or keep member records overnight at a personal residence if they have completed the BAC approved *data safeguarding form* (HHSA 23-26) and follow the applicable BAC Policy and Procedures (HHSA L-26). Contracted workforce members should develop their own policies and procedures that comply with Article 14 and State Agreement requirements.
- Programs should only remove member information from program offices for approved business purposes, with prior management approval, and information shall be stored in an appropriate manner.
- Programs shall sign in and out records, as needed.
- When saving member contact information on an encrypted device, such as a phone or laptop, or transporting member information out of the office/clinic, only include the minimum member identifying information necessary.
- Member information must not be stored on a non-encrypted device.
- No workforce staff may ever leave member information unattended in a car for any amount of time.

For more information and details for all sections below, please see: HHS.GOV-Your Rights Under HIPAA.