B. 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.

COMPLIANCE

County Programs

- As part of this commitment, all County Mental Health Services workforce members[1] shall be familiar with and adhere to Agency Compliance Office (ACO) policies and procedures. In addition, County Mental Health Programs shall have processes that ensure adherence to the HHSA Code of Conduct. All ACO policies and procedures, including the Code of Conduct, may be found on the ACO website.

Contracted Programs

- 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 (annual) in agreements with the County must have a Compliance Program that meets the Federal Sentencing Guidelines,[2] including the seven elements of an effective compliance program, which are:

    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.

[1] Workforce members include employees, volunteers, trainees, and other persons whose work are under the control of the Program, and/or pertain to the applicable County contract, regardless of whether the individual is paid for their work.

[2] Federal Sentencing Guidelines section 8B2.1 and 42 CFR 438.608(b)(1) – (b)(7)

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

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:

    1. All new employees shall receive a thorough employee orientation about compliance requirements prior to employment.

    2. Staff shall have proper credentials, experience, and expertise to provide client services.

    3. Staff shall document client encounters in accordance with funding source requirements and HHSA policies and procedures.

    4. Staff shall bill client services accurately, timely, and in compliance with all applicable regulations and HHSA policies and procedures.

    5. Staff shall promptly elevate concerns regarding possible deficiencies or errors in the quality of care, client services, or client billing.

    6. Staff shall act promptly to correct problems if errors in claims or billings are discovered.

BHP's Compliance Hotline

- Concerns about ethical, legal, and billing issues, whether pertaining to a County or Contracted Program, may be raised directly to the ACO at 619-338-2807 or Compliance.HHSA@sdcounty.ca.gov, as well as Compliance Hotline at 866-549-0004.

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, the State licensing board, or your professional association.

Documentation Requirements

- All County and Contracted Programs are required to prepare and maintain appropriate medical records on all clients receiving services in compliance with Title 9, Chapter 11 and 42 CFR guidelines. Programs are expected to meet all documentation requirements and standards established by the Behavioral Health Plan (BHP) in the preparation of these records. The MHP has the responsibility to prepare and maintain the Uniform Clinical Record Manual (UCRM), which outlines the MHP's requirements and standards in this area. Both the UCRM and the SDCBHS Management Information System User Manual, which contains the requirements for the most commonly used services, are available at the Optum Website.

- Many of the requirements present in the BHP's UCRM are derived from the BHS contract with the California Department of Health Care Services (DHCS) to provide specialty mental health services (State Agreement). Other documentation requirements have been established by the BHP's Uniform Medical Record Committee, which is an ad hoc committee chaired by QA.

- In order to ensure that programs are knowledgeable of documentation requirements, QA provides the following:

    - Annual Quality Assurance Forum for all System of Care (SOC) providers presented by the QA, PIT, and MIS units. Information is presented on system wide compliance with State, Federal and County BHP requirements. Areas for continuous quality improvement are identified and implemented for the System of Care.

    - Quarterly in-service documentation training for all new clinical staff, or any clinical staff that may need a documentation review.

    - On-site in-service trainings tailored to program's specific documentation training needs when requested by the program or identified by QA.

Claiming and Reimbursement of Mental Health Services

- All rendering providers of specialty mental health services shall have a National Provider Identification (NPI) number prior to claiming for services. All providers are required to obtain NPI number as part of their staff account set up in the electronic health record. Providers may contact the MHMIS unit for questions.

- When providing reimbursable mental health services, providers are required to utilize all available payor sources appropriate for reimbursement of services. Many clients have one or more insurance sources (e.g., Medicare, indemnity, PPO, HMOs, Medi-Cal) and it is the responsibility of each program to appropriately bill and collect reimbursement from primary and secondary insurance sources.

- For all clients receiving mental health services, programs are required to be aware of all available payor sources, be able to verify eligibility and covered benefits, obtain an Assignment of Benefits (AOB), track and process Explanation of Benefits (EOBs) and primary insurance denials, in order to seek reimbursement from secondary payor sources. All billing and submission of claims for reimbursement must be in accordance with all applicable County, State and Federal regulations.

- For detailed guidelines and procedures regarding insurance billing, claims processing, assignment of benefits, determining eligibility, and accounts collection and adjustment, please refer to the Financial Eligibility and Billing Procedures - Organizational Providers Manual.

Coding and Billing Requirements

- The Health Insurance Portability and Accountability Act (HIPAA) include requirements regarding transactions and code sets to be used in recording services and claiming revenue. UCRM forms reflect the required codes, and County QA staff provide training on the use of the Service Record forms.

- Additional requirements come from the State Agreement; these requirements determine the nature of chart reviews during a Medi-Cal audit and the items for which financial recoupment of payment for services will be made by State or County reviewers.

- Following are current requirements and resources related to coding and billing:
    - Services must be coded in compliance with the Management Information System User Manual, Organization Provider Operations Handbook (OPOH) and the Financial Eligibility and Billing Manual.

    - Diagnoses must be coded using the International Classification of Diseases (ICD-10). In general, a diagnosis is made using the fuller descriptions of the Diagnostic and Statistical Manual, and "cross-walked" to the correct service code for SmartCare by the clinician. The service code should result in the highest level of specificity in recording the diagnosis.

    - Services are recorded in the EHR through service note entry or if done on paper on the corresponding downtime form and maintained in the hybrid chart If completed on paper, the document may be scanned into the EHR and viewed on the "Documents (Client)" page but is not required. The program should follow the Administrative Service Entry instructions.

- Documentation standards associated with coding and billing requirements can be found in the OPOH, *Section G*, UCRM, Financial Eligibility and Billing Manual, and the CPT Crosswalk, all located on the Optum website > BHS Provider Resources> SMH & DMC-ODS Health Plans page.

False Claims Act

- The Federal False Claims Act[3] (FCA) helps the government combat fraud in federal programs, purchases, and contracts. The California False Claims Act[4] (CFCA) 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 or duplicate billing

- County and County Contracted Programs are required to promptly report circumstances that may affect the member's eligibility such as the death of a member to the California Department of Health Care Services (DHCS). in addition to notifying the DHCS, the County or County Contracted Programs shall conduct an internal investigation to determine the validity of the issue/complaint, and develop and implement corrective action, if needed.

- The CFCA 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.

- Any indication that any one of these activities is occurring should be reported immediately to the ACO at 619-338-2807, Compliance.HHSA@sdcounty.ca.gov, or to the HHSA Compliance hotline at (866) 549-0004. If any County or Contracted program needs training on the False Claims Act, reach out to the ACO 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.

Medi-Cal Fraud Complaint – Intake Unit Audits and Investigations
1-800-822-6222

[3] 31 U.S.C. §§ 3729-3733.
[4] CA Gov't Code §§ 12650-12655.

fraud@dhcs.ca.gov
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 beneficiaries and that services meet criteria for access to SMHS and the services were medically necessary. Programs shall complete service verification as outlined in their P&P. If discrepancies are found during the service verification process, the program will complete the require reporting and corrections as outlined in their P&P.

- Program Integrity includes:
  - Accurate eligibility determination
  - Services provided are medically necessary and appropriate
  - New/current providers are not on the excluded provider list(s)
  - Verify with the member that services reimbursed by Medi-Cal were received by client
  - Immediate and corrective actions upon discovery that services paid/claimed by Medi-Cal were not received by client(s)

- Service Verification includes services which have been claimed and reimbursed by Medi-Cal

- Service verification activity documents **may** include:
  - Service reports from EHR
  - Verification letters with client signature
  - Client sign in sheets
  - Signature logs
  - Call logs with attestation

- 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 Quality Assurance Program Reviews (QAPR). QA tracks and monitors

results of Quality Assurance Program Reviews and may require a program to develop a Quality Improvement Plan (QIP) to address specific documentation concerns.

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.[5]

BHP Responsibilities

- In order to ensure compliance with applicable privacy laws as well as the State Agreement, the BHP has the following requirements for County and Contracted Programs. Programs are responsible for ensuring compliance with the latest requirements within the State Agreement, which can be found at the HHSA Business Assurance and Compliance website. If any County or Contracted provider has questions about privacy or security requirements, reach out to the ACO at 619-338-2808 or privacyofficer.hhsa@sdcounty.ca.gov. As of 2018, some, but not all of the requirements include that all workforce members shall:

    - Be trained on privacy and security of client 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 years. Training must be provided within a reasonable period of time upon hire and at least annually thereafter. If any County or Contracted program needs assistance with privacy and security training, reach out to the ACO at 619-338-2808 or privacyofficer.hhsa@sdcounty.ca.gov.

    - Sign a confidentiality statement prior to provision of client information. 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 and retention for six years.

    - Only access client records as necessary to perform their jobs

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

[5] Applicable privacy laws include, but are not limited to, 45 CFR 164 (Health Insurance Portability and Accountability Act or HIPAA), CA Civil Code 56 (California Confidentiality of Medical Information Act), 5 U.S.C. § 552a (the Privacy Act of 1974) CA Civil Code 1798 (California Information Privacy Act), U.S.C 38 §7332 (Veterans Benefits), CA W&I Code 10850.1 (Multi-Disciplinary Teams).

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[6] to make treatment decisions on behalf of the client. A client acknowledgement of the NPP is maintained in the EHR and/or the hybrid chart. 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 ACO website.

- Contracted Programs may, but are not required, to use the HHSA NPP located on the Optum Website> BHS Provider Resources > SMH & DMC-ODS Health Plans> *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 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.

Uses and Disclosures of Records

- The County of San Diego BHS manages an electronic health record (EHR) for the BHP County and Contracted providers. The EHR holds client's protected health information (PHI) which is accessible by County and Contracted providers to improve coordination of care across the BHP System of Care. PHI documented within the EHR is also used for internal County operation purposes.

- When a third-party requests client information, the Program should ensure compliance with applicable privacy laws. When accepting an authorization form from an outside source, programs shall reasonably ensure the authorization is valid and verify the identity of the requestor before providing client information. County Programs shall follow the relevant ACO policies and procedures (HHSA L-25 and HHSA L-09). County Programs shall also use the HHSA-approved authorization form (HHSA 23-09) when soliciting client records from a third party.

- Contracted Programs may, but are not required, to use the HHSA Authorization form located on the Optum Website > BHS Provider Resources > SMH & DMC-ODS Health Plans> *UCRM* tab.

[6] For County programs, a definition of Authority may be found at ACO Policy and Procedure HHSA L-27.

- 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 an authorization policy and a Uses and Disclosures policy to ensure these requirements are followed by workforce members.

- If the third-party request solicits information from multiple legal entities, the Program that received the request should promptly inform the requestor of the contact information for the other entities so the requestor can make those subsequent requests.

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 ACO 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 as well as other information regarding privacy policies and procedures can be located on the HHSA County Compliance Office Website- Privacy Policies, Procedures and Forms

- 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.

- The BHP County and Contracted providers may only charge a reasonable fee which can only include costs for labor associated with copying, supplies, postage, or preparation of summary as agreed to by client. In any case, clients may not be charged more than $.25/page for copies and $.50/ page for microfilm.

- **Client Requests to Multiple Legal Entities**

    - If the client request pertains to multiple legal entities, the Program that received the request should promptly inform the requestor of the contact information for those other entities so the requestor can make those subsequent requests.

- County or Contracted provider may deny a client's request for records provided that a licensed healthcare professional has determined that the access requested is reasonably likely to endanger the life or physical safety of the client or another person. The client must be given the right to have such denials reviewed by a licensed health care professional who is designated by the BHP to act as the reviewing official and who did not participate in the original denial.

- The BHP delegates the independent review to each contracted legal entity. Each legal entity must provide or deny access in accordance with the determination of the reviewing official. Each contracted legal entity is required to have a policy and procedure that identifies the independent review process.

Client Requests for Amendment and Client Requests for Accounting of Disclosure

- When a Program receives a request to amend SmartCare records and believes amendments need to be made, or when a Program receives a request for an accounting of disclosures of SmartCare records, the program should contact the SDCBHS MIS team 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.

Handling/Transporting Medical Record Documents

- To maintain the confidentiality and security of client records, all Programs will securely store and transport medical records, including laptops, phones, and tablets which may contain client identifying information in accordance with applicable laws and the State Agreement, including, but not limited to, the below:

    - Client records must be maintained at a site that complies with Article 14 requirements, including the current State Agreement. This means no client information may be left at a site unless that site has a contract with the County that includes Article 14. If a program is unsure, they should check with their Contracting Officer's Representative (COR).

    - County workforce members may, as needed, transport client records and/or keep client records overnight at a personal residence if they have completed the ACO approved *data safeguarding form* (HHSA 23-26) and follow the applicable ACO 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 client 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 client contact information on an encrypted device, such as a phone or laptop, include the minimum client identifying information necessary. Remember that even identifying an individual as receiving mental health services is protected information. Client information should not be stored on a non-encrypted device (such as a flip phone).
- No workforce member may ever leave client information unattended in a car, even if the records are in a locked box, and/or inside a locked trunk, and/or it's only for a few minutes.
- When transporting client information out of the Program office or clinic, include only the minimum client identifying information needed.

Privacy Incidents

- A privacy incident[7] 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 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 ACO policies and procedure (L-24).

[7] For formal definition, County Programs may see ACO Policy L-30. Contracted Programs may review their Article 14.

All programs shall immediately notify the ACO Privacy Officer and COR via email, complete the ACO approved *Privacy Incident Report* (HHSA 23-24), and send it within one (1) business day to the ACO Privacy Officer and COR via email. All of these documents can be found at the HHSA Business Assurance & Compliance website. Contracted Programs must additionally ensure compliance with HIPAA breach requirements, such as risk analysis and federal reporting and inform the ACO of any applicable requirements.

Privacy Incident Reporting (PIR) for Staff and Management

1. Staff becomes aware of a suspected or actual privacy incident.
2. Staff notifies Program Manager immediately.
3. Program Manager notifies County COR and County Privacy and Compliance Officer immediately upon knowledge of incident.
4. Program Manager completes and returns an initial HHSA Privacy Incident Report (PIR) (located on the HHSA Business Assurance & Compliance website) to the County COR and County Privacy and Compliance Officer within one (1) business day.
5. Continue investigation and provide daily updates to the County Privacy and Compliance Officer.
6. Provide a completed HHSA Privacy Incident Report (PIR) to the County COR and County Privacy and Compliance Officer within seven (7) business days.
7. Complete any other actions as directed by the County Privacy and Compliance Officer.

- San Diego County 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.