

COUNTY OF YOLO

HEALTH AND HUMAN SERVICES AGENCY

POLICIES AND PROCEDURES

SECTION 5, CHAPTER 4, POLICY 002

CONFIDENTIALITY AND PRIVACY OF BEHAVIORAL HEALTH CLIENT INFORMATION

A. PURPOSE:

1. To establish Yolo County Health and Human Services Agency (HHSA) responsibilities for maintaining confidentiality of client information in the operation of its behavioral health programs, including mental health and substance use disorder programs.
2. To assure all applicable County, State and Federal laws, rules and regulations pertaining to confidentiality are appropriately incorporated into HHSA behavioral health operations.
3. To assure all pertinent sources of information within the purview and responsibility of HHSA behavioral health programs are maintained and shared in accordance with all applicable confidentiality policies, regulations, and laws.

B. FORMS REQUIRED/ATTACHMENTS:

- Attachment 5-4-002A: *Guidance Regarding the Confidentiality and Privacy of Client Information for Behavioral Health Services Employees and Contractors;*
- Form 5-4-002A: *Confidentiality and Privacy Agreement for Behavioral Health Services Employees and Contractors;*

C. DEFINITIONS:

1. **Client Information:** is information maintained in any format, such as paper, electronic mail, computerized information systems, photographs, audio and video recordings communication with media and other verbal and non-verbal (gesturing, etc.) communication, and includes:
 - a. **Department Personal Information (DPI):** which is defined as personal information accessed in a database maintained by the Department of Health Care Services (DHCS), received by HHSA from the DCHS or acquired or created by HHSA in connection with performing the functions, activities and services specified in the State Agreements on behalf of the DCHS.
 - b. **Personal Information (PI):** which is defined as any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.

- c. **Personally Identifiable Information (PII):** which is defined as any information that can be used to distinguish or trace a consumer's identity (e.g., his or her name, Social Security Number, biometric records) alone or when combined with other personal or identifying information that is linked or linkable to a specific consumer (e.g., date of birth, place of birth, mother's maiden name).
 - d. **Protected Health Information (PHI):** which is defined as individually identifiable health information that is created or received by a health care provider, health plan, employer, or health care clearinghouse and that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual.
2. **Access:** The inspection or copying of client information maintained by HHSA.
 3. **Use:** The sharing, employment, application, utilization, examination, or analysis of client information within HHSA, its affiliates, or its contract providers.
 4. **Disclosure:** To release, transfer, provide access to, or divulge in any other manner client information outside of HHSA.
 5. **Authorization:** The formal consent document releasing client information from the records of an entity covered by the privacy provisions of HIPAA and other Federal and State law and regulations.
 6. **Behavioral Health Employee:** For purposes of this policy, the term "Behavioral Health Employee" (BH employee) is used broadly and is defined to mean any permanent or temporary employee, temporary agency or locum tenens employee, persons employed under contract or purchase of service agreement, unpaid students, interns, volunteers and any other persons who assists HHSA with the provision of behavioral health services in the course of their work duties.
 7. **Behavioral Health Contractors:** For purposes of this policy, the term "Behavioral Health Contractor" (BH contractor) means any contracted provider that performs a contracted scope of services that assists HHSA with the provision of behavioral health services, including any permanent or temporary employee, temporary agency or locum tenens employee, persons employed under contract or purchase of service agreement, unpaid students, interns, volunteers and any other persons who assist the provider.

D. POLICY:

1. HHSA behavioral health programs shall ensure and protect the privacy and confidentiality of all sources of client information in accordance with all applicable Federal and State laws and regulations and in compliance with all Yolo County and HHSA policies and procedures, including but not limited to:
 - a. All information and records obtained in the course of providing services to voluntary and involuntary recipients of specified services, including mental health, community mental health, admissions and judicial commitments to mental institutions. (Cal. Welf. & Inst. Code §5328.)

- b. All PHI as specified in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). (45 C.F.R §§160.103 & 164.500.)
 - c. All PI as specified in the California Information Practices Act. (Cal. Civ. Code §1798.3.)
 - d. All PII and Department PI as specified in the Agreements between the DHCS and Yolo County, including the Mental Health Plan Agreement regarding the provision of specialty mental health services and the Substance Use Disorder Agreement regarding the provision of Drug Medical and Non-Drug Medi-Cal substance use disorder services.
2. BH employees and BH contractors shall take responsibility to ensure they understand and use current and relevant confidentiality laws, regulations and guidelines regarding client information as they apply to their job responsibilities and duties and/ or contracted obligations.
 3. Confidentiality of client information shall be assured without compromising applicable legal rights of access for information by any appropriate party, including employees, clients, family, professionals and agencies or other pertinent groups.
 4. HHS Behavioral Health Program/Unit Managers and Supervisors shall be responsible for enforcing all confidentiality policies, laws, and regulations within his/her scope of responsibility. BH contractors shall delegate oversight to appropriate personnel in their entity/organization.

E. PROCEDURE

1. All BH employees and BH contractors shall be provided with a copy of the HHS Behavioral Health Code of Conduct (BH Code of Conduct.) All BH employees and BH contractors shall review the BH Code of Conduct in its entirety. BH employees and BH contractors are expected to understand and abide by the contents of the BH Code of Conduct and shall sign an attestation stating same.
2. All BH employees shall be provided with guidance regarding the confidentiality of client information entitled *Guidance Regarding the Confidentiality and Privacy of Client Information for Behavioral Health Services Employees and Contractors* (BH Client Confidentiality Guidance) attached hereto as Attachment 5-4-002A. All BH employees and BH Contractors shall review the BH Client Confidentiality Guidance in its entirety. BH employees and BH contractors are expected to understand and abide by its contents and shall sign the *Confidentiality and Privacy Agreement for Behavioral Health Services Employees and Contractors*, attached hereto as Form 5-4-002A.
3. The completed and signed *Confidentiality and Privacy Agreement for Behavioral Health Services Employees and Contractors* forms (Form 5-4-002A) will be maintained by the HHS Behavioral Health Quality Management Unit.
4. BH employees and BH contractors shall only access or use client information on a "need to know" basis. This shall include, but not be limited to, use and storage of passwords in a manner that assures they are not shared with unauthorized persons.

5. Release of client information to any party shall be carried out only upon completion of a valid and current written authorization for use and disclosure or when release without client/legal representative consent is legally mandated by or is otherwise legally authorized.
6. Situations mandating release of information with or without consent include, but are not limited to, the following:
 - a. By a mandated reporter who has knowledge of or observes a child in his/her professional capacity or within the scope of his/her employment whom he/she knows or reasonably suspects has been the victim of child abuse or neglect. (Cal. Pen. Code §11166.)
 - b. By a mandated reporter who encounters suspected elder or dependent adult abuse or neglect. (Cal. Welf & Inst. Code §15630.)
 - c. When the patient, in the opinion of his/her psychotherapist, presents a serious danger to a reasonably identified victim or victims. (Tarasoff Decision).
 - d. Upon the receipt of a properly served subpoena. See HHSAs Policies and Procedures re Proper handling of Subpoenas, for specific procedures.
7. BH employees shall consult with their Program/Unit Managers and Supervisors or the Behavioral Health Compliance Officer regarding specific confidentiality matters. BH contractors shall delegate oversight to appropriate personnel in their entity/organization but should also reach out to the Behavioral Health Compliance Officer as needed.
8. Even though HHSAs behavioral health service delivery systems (e.g., substance use disorder & mental health services) are a part of a quality continuum of care, BH employees and BH contractors shall maintain confidentiality of client information as required with all applicable statutes and regulations.

While HIPAA provides for the disclosure of confidential information for treatment purposes, other applicable laws are more restrictive. For example, if there is not a valid and current authorization for use and disclosure and the disclosure is for treatment purposes:

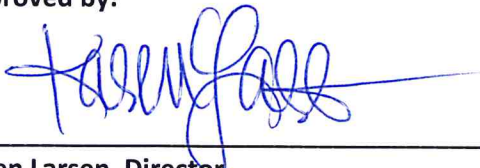
- a. a client's information and records re substance use disorder and services may **ONLY** be shared within the substance use disorder treatment team that is currently treating the client. (42 CFR Part 2 Final Rule.)
 - b. a client's information and records re mental health condition and services may **ONLY** be shared between qualified professionals in the provision of services if providers have "medical or psychological responsibility for the patient's care." (Cal. Welf. & Inst. Code §5328.)
9. BH employees and BH contractors are strictly prohibited from using confidential information and records relative to HHSAs behavioral health clients in connection with outside work or business interests. Confidential information possessed by HHSAs behavioral health programs and required by professional clinicians in carrying out private services to clients shall only be shared through appropriate and legally compliant channels.

10. BH employees and BH contractors shall also apply all pertinent confidentiality guidelines to documents not typically included in a clinical record, such as telephone calls to the Access line or Patients' Rights, and interpreter services, as well as, all information maintained in computer or hand tally databases/logs, such as telephone numbers, names, addresses and social security numbers.
11. BH employees and BH contractors shall follow the appropriate procedures for maintaining confidentiality in the reporting of incidents involving injuries, deaths and alleged patient abuse.
12. BH employees and BH contractors shall assure that client records are distributed, maintained and stored in a manner that will assure access only to those persons authorized to review records. Each HHSA Behavioral Health Program/Unit Managers and Supervisors shall regularly monitor operations to assure client records are distributed and secured in a manner that will assure confidentiality. BH contractors shall delegate oversight to appropriate personnel in their entity/organization. That appropriate personnel shall regularly monitor operations to assure client records are distributed and secured in a manner that will assure confidentiality.
13. Confidentiality of HIV and AIDS information as it pertains to HHSA behavioral health clients shall be maintained in keeping with HHSA Policies and Procedures re Human Immunodeficiency Virus (HIV) and Acquired Immunodeficiency Syndrome (AIDS) Clinical Documentation and Confidentiality.
14. Information stored in electronic data systems shall be maintained in keeping with all applicable confidentiality regulations.

F. REFERENCES

1. Cal. Welf. & Inst. Code §§5328, 15630
2. 45 CFR §§160.103 & 164.500.
3. Cal. Civ. Code §1798.3.
4. Cal. Pen. Code §11166.
5. *Tarasoff v. Regents of the University of California* (1976) 17 Cal. 3d 425
6. 42 CFR Part 2 Final Rule

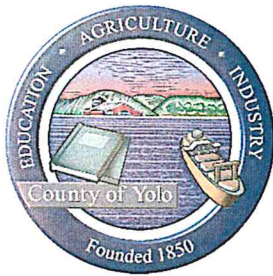
Approved by:



Karen Larsen, Director
Yolo County Health and Human Services Agency

11/13/17

Date



COUNTY OF YOLO

HEALTH AND HUMAN SERVICES AGENCY

POLICIES AND PROCEDURES

GUIDANCE REGARDING THE CONFIDENTIALITY AND PRIVACY OF CLIENT INFORMATION FOR BEHAVIORAL HEALTH SERVICES EMPLOYEES AND CONTRACTORS [HHS ATTACHMENT 5-4-002A]

I. INTRODUCTION

As employees and contractors of a healthcare system, we are entrusted to protect the information with which we work. In your job, you may come into contact with client or consumer health information, other personal information about clients or consumers, financial information, employee and payroll information and business information considered to be confidential by the County of Yolo and the Yolo County Health and Human Services Agency (HHS). Many of our programs are required to enter, access or use information that is considered to be California State "Department PII". It is critically important that you protect any confidential information that should not be disclosed to unauthorized individuals or entities. In addition to not disclosing confidential information, you must also take reasonable steps to ensure that the confidential information that you receive, regardless of its format, is protected from theft or unauthorized access. Our collective effort to ensure the privacy and security of confidential information upholds our core values, demonstrates respect for our clients, and supports compliance with State and Federal laws. Your commitment to protecting our confidential information is an element of our success.

Note: While this document will focus primarily on Protected Health Information and Personally Identifiable Information, the principles will apply to all confidential information that you work with.

II. BRIEF OVERVIEW OF HEALTH INFORMATION PRIVACY AND SECURITY REGULATIONS

A. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA was created by the federal government to promote improvements and efficiencies in the provision of health care. A major goal of HIPAA was to protect the privacy and security of health information. HIPAA regulations include the following parts:

- **Privacy.** The privacy regulations govern who has access to Protected Health Information (PHI). They ensure that PHI is used appropriately by creating a national minimum standard of privacy (state laws can be more stringent). The privacy regulations also give clients specific rights regarding their own health information.
- **Security.** The security regulations govern how health information is protected. They establish safeguards for PHI.

B. Other Laws

While we regularly refer to HIPAA regulations, other state and federal regulations govern the privacy and security of health information and other personal information. These regulations are the ones that most often regulate our County work: 42 CFR Part 2 (governing Substance Use Disorder patient records), Welfare and Institutions Code Section 5328-5830 (governing mental health client information) and Civil Codes Sections 1798.29, 1798.82 and 1798.84 (regulating the privacy of personal information), and the CA Confidentiality of Medical Information Act - Civil Code, Sections 56-56.37.

Also, in order to have continued access to Medi-Cal PII and MEDS, the Social Security Administration (SSA) required the California Department of Health Care Services (DHCS) to enter into a Medi-Cal Data Privacy and Security Agreement with all 58 California Counties. The agreement requires each County to meet SSA, State and Federal security requirements to ensure the confidentiality and security of Medi-Cal PII and to limit MEDS access to those employees who need it to perform their official duties.

III. OVERVIEW OF BASIC CONCEPTS

A. What is Protected Health Information (PHI)?

PHI is a type of Personally Identifiable information (PII) related to a person's health care treatment and/or to the corresponding payment for those services. PHI includes information that could reasonably identify an individual (client identifiers) and is connected to their sensitive health information. PHI in electronic, paper, or oral forms must be protected. Every member of the work force, even those who don't deal directly with client information, should have an understanding of what PHI is and the ways in which it must be protected. PII is similar to PHI and must also be protected. PII differs from PHI in that it not necessarily health information.

- **Client Identifiers:** Names, street address, city, county, full zip code (with some qualifications), dates directly related to an individual (e.g. birth date, dates of service), telephone and fax numbers, email addresses, Social Security numbers, credit card numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers, internet protocol (IP) addresses, biometric identifiers (e.g. finger and voice prints), full-face images, and any other unique identifying number, characteristic, or code.
- **Examples of Sensitive Health Information:** Diagnoses, Procedures, Medications, Physician name and specialty, Location of service (e.g. cancer center), Service type (e.g. physician office, radiology, inpatient admission), Test results, Amount charged and paid.

B. Use of PII/PHI, Generally

Employees and contractors may potentially use PII/PHI daily to provide critical healthcare services to our clients. Generally, PII/PHI can be used and shared by a client's direct treatment team to provide healthcare services and for other operational purposes such as billing. When

used properly, PII/PHI supports positive outcomes in the healthcare services we provide. The permitted uses of PII/PHI differ slightly depending on the type of healthcare being used or reviewed. The terms of the contract and the laws a regulation regarding the type of services that are provided will specify the appropriate uses for different types of confidential information.

C. Need to Know/Minimum Necessary

You should only access PII/PHI based upon your having a “need to know,” i.e., when the information relates to your official duties. Limit your access to only that PII/PHI which is needed for you to do your job.

The law requires that organizations take reasonable steps to allow access only to the minimum PII/PHI necessary to perform a specific task or job. This minimum necessary standard applies to both internal uses as well as external disclosures. Contractors and external providers must only request and receive information tailored to the specific task or job. It is important that you do not access, use or disclose more confidential information than you are authorized to access and that you need to complete your job. The minimum necessary standard is not intended to impede client care and therefore it is important to understand when and in what circumstances it is appropriate and legally permissible to share PII/PHI.

D. Breach of PII/PHI

Generally, there are “permitted” uses and disclosures of PHI/PII and “impermissible” uses or disclosures of PHI/PII. A breach is presumed when you use or disclosure PHI/PII in a manner not permitted by policy or law. A breach can be deliberate or accidental. Our goal as community partners, entrusted with confidential client and business information, is not to commit a breach of that confidential information. While our goal is to have no breaches, we understand that there may be times when a mistake is made and you access, use or disclose PHI, PII or other confidential information improperly. When or if this happens, it is our policy and the law that you immediately tell your supervisor and/or the HHS Behavioral Health Compliance Officer that you suspect there may have been a breach. NOTE: The best way to prevent a breach is to ask a supervisor or HHS Behavioral Health Compliance Officer PRIOR to access, use or disclosure if you are unsure about whether you are authorized and/or whether you are using the correct procedures/safeguards.

E. Disclosure of PII/PHI

While you may access and use PHI/PII as part of your duties, you may also be asked to disclose PHI/PII to others for a variety of reasons. There are a few permitted reasons that you may disclose PHI/PII to others without a client’s written permission or authorization. Permitted disclosures without authorization may include: discussing a client’s own information with, or providing a copy of the information to the client. Healthcare providers may also disclose PHI without a client’s authorization for the purposes of treatment, payment or healthcare operations. The rules for disclosing PHI vary depending on the type of healthcare provider or the type treatment provided, for example Substance Use Disorder services are specifically protected by federal law and you should familiarize yourself with policies and regulations that apply to your area of work, prior to disclosing any confidential information. In addition, always ask your

supervisor or the HHS Behavioral Health Compliance Officer for guidance if you are unsure about the permitted reasons for disclosures.

F. Authorization

Generally, PHI may be used in a healthcare environment for treatment, payment or healthcare operations. A written authorization from the client is required for many uses and disclosures that fall outside of treatment, payment or healthcare operations. HHS has a form that a client may use, but occasionally another entity will present an authorization from the client requesting our records. Generally, no other forms will be accepted. Occasionally, exceptions will be made only after a form is determined to be authentic and complete is the sole discretion of the BH Compliance Officer. It is important that no PHI/PII is disclosed unless the authorization form is determined to be authentic and complete. Once an authorization is signed, a client has the right to revoke or cancel it at any time. HIPAA specifically states that care cannot be conditional upon a client's signing of an authorization. Until you are trained on the policies and procedures pertaining to disclosure of PHI or other confidential information in your area of work, you should request assistance from your supervisor.

G. Compliance with Policies and Procedures

Be familiar with HIPAA privacy and security policies and procedures. The County of Yolo and HHS have policies on privacy and security of personal and health information. You will be informed of new or revised policies and will be expected to read, understand and acknowledge the policies. Ask your supervisor for details of any specific policies or procedures that relate to your work.

IV. SAFEGUARDS

- A.** The law requires HHS to implement and maintain appropriate safeguards to protect PII/PHI from unauthorized access, use and disclosure. Safeguards you must use and support include:
- 1.** PII/PHI may only be used, accessed, or disclosed for administration of HHS behavioral health services programs. Never access or look at a client record that you do not have permission and a business need to see. Only access the minimum amount of information necessary for you to complete your duties.
 - 2.** Never discuss a client (even the existence of a client) with anyone outside of the authorized treatment or operations team. (This can be one of the most common and damaging forms of breach). If unsure who you may discuss a client with, ask for guidance from a supervisor.
 - 3.** Always create strong passwords for system access and never share any of your passwords with anyone. Do not ask others to use their passwords.
 - 4.** Always lock your computer (ex. Window key+L) when you leave it unattended for even a minute. Ensure that no one can watch you logon and that those who

are not authorized cannot see your computer screen when you are viewing confidential information.

5. Ensure your computer automatically locks, requiring a password to unlock, after no more than five (5) minutes of inactivity.
6. Safeguard the placement of computers, printers, and fax machines to limit potential access by unauthorized users. Retrieve documents from printers and fax machines immediately.
7. Any computer accessing or storing PII/PHI must be encrypted to prevent access in case of loss or theft.
8. You may not access or store PII/PHI via any mobile device (cell phone, laptop, tablet, kindle, flash drive, etc.) For example, you must never download PII/PHI on a compact disk or an unencrypted flash drive.
9. You must ensure that all confidential information in paper form is always in your direct control or is locked in a secure location where it can be accessed only by authorized users. Dispose of confidential paper through shredding or by placing the item in locked, confidential recycling bins.
10. Secure all client credit information. Do not leave receipts or files containing client information including credit card numbers in an unsecured manner. If you must temporarily write down a client credit card number or social security number, be sure to shred the paperwork after you are finished using it.
11. All electronic communication containing County information must include a confidentiality statement. Do not open suspicious attachments to e-mails, they may contain viruses or malware intended to steal confidential information or password credentials.
12. Do not download or install software on county property without permission from the HHSA IT Department.
13. All PII/PHI sent via e-mail outside of the County e-mail system must be encrypted. Never include confidential information in the subject line of an e-mail.
14. Do not open suspicious attachments to e-mails, they may contain viruses or malware intended to steal confidential information or password credentials.
15. You must ensure that any PII/PHI transmitted electronically, (fax, e-mail, voicemail) is appropriately protected pursuant to HHSA policy and you must double check that the fax number, phone number, or e-mail ID is correct. (This is one of the most common reasons for breach). Call ahead to verify the fax

number or e-mail and let the person to whom you are sending the information know when to expect the PII/PHI.

16. Verify the identity of anyone requesting confidential information. If discussing PHI over the phone ensure you recognize the client's voice or you ask identifying questions that the client would know (for example, last 4 of SSN, middle name, address etc.)
17. You must be aware of your surroundings when having verbal conversations about confidential information. Do not have conversations in hallways, break rooms, cubicles, or other places where others may be able to hear. Unpermitted disclosure through someone overhearing a conversation is still a breach.
18. If you overhear a confidential conversation in a public hallway or elevator, ask the individuals to move to a private location to continue the discussion.

IV. COMPLAINT PROCESS

If you need to report a suspected breach or if you want information about confidentiality and privacy practices, you should work with your supervisor or manager. If that is not reasonable or appropriate, you can call the HHS Behavioral Health Compliance Officer at 1 (800) 391-7440. Reports made to this number are not anonymous but will be kept confidential to the greatest extent possible.

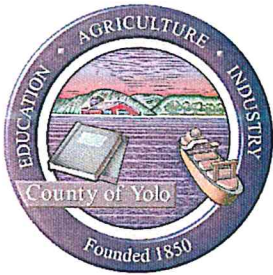
If you would like to make an anonymous complaint, please mail it to:

Attn: HHS Behavioral Health Compliance Officer
137 N. Cottonwood. St. #2611
Woodland, CA 95695

Please remember, employees and contractors are required by law and contract to report any breach or suspected breach they may become aware of. This includes breaches made by yourself or other employees, either accidentally or negligently.

V. ENFORCEMENT

Employees and contractors who access, disclose or use PII/PHI in a manner or for a purpose not authorized by may be subject to civil and criminal penalties, including fines and/or imprisonment. HHS is required by law to apply appropriate sanctions against employees and contractors in violation of this policy, up to and including employment or contract termination.



COUNTY OF YOLO

HEALTH AND HUMAN SERVICES AGENCY

POLICIES AND PROCEDURES

CONFIDENTIALITY AND PRIVACY AGREEMENT FOR BEHAVIORAL HEALTH SERVICES EMPLOYEES AND CONTRACTORS [HSA FORM 5-4-002A]

GENERAL USE:

It is the legal and ethical responsibility of all County behavioral health employees, contractors, and volunteers to use personal and confidential client, employee and County business information (referred to here collectively as "Confidential Information") in accordance with; the law, Yolo County policy, Yolo County Health and Human Services Agency (HHSA) policy, and/or contract, and to preserve and protect the privacy rights of the subject of the information as they perform their duties.

Confidential Information includes, but may not be limited to: any information that identifies an individual, written records or electronic records contained in systems to which behavioral health employees, volunteers, interns and/or contractors, have been provided access.

Laws controlling the privacy of, access to and maintenance of confidential information include, but are not limited to, the Federal Health Insurance Portability and Accountability Act (HIPAA), the Information Practices Act (IPA), the California Confidentiality of Medical Information Act (CMIA), the Lanterman-Petris-Short Act (LPS) and Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2 – known as "Part 2") These and other laws apply whether the information is held in electronic or any other form or format, and whether the information is used or disclosed orally or in writing. Confidential information may be used and disclosed only in the performance of assigned duties for the purpose of providing services. The HHSA Behavioral Health Confidentiality and Privacy of Behavioral Health Client Information, 5-4-002 is hereby incorporated by reference.

UNACCEPTABLE/INAPPROPRIATE USE:

Workforce members may not share or disclose confidential information with unauthorized individuals including, but not limited to, family, friends, acquaintances, or other County behavioral health employees absent a legitimate business reason (i.e., the disclosure is related to the provision of services to the client) or the client has provided written authorization for the disclosure.

ENFORCEMENT POLICIES:

Behavioral health employees and contractors who access, disclose or use PII/PHI in a manner or for a purpose not authorized by law may be subject to civil and criminal penalties, including fines and/or imprisonment. HHSA is required by law to apply appropriate sanctions against behavioral health employees and contractors in violation of this policy, up to and including employment or contract termination.

For behavioral health employees, disciplinary action, up to and including termination, may be imposed if a client's confidentiality is violated in accordance with the laws, regulations, or County policies. For behavioral health contractors, action will be taken, up to and including terminating the relationship and services, if a client's confidentiality is violated. In addition, behavioral health contractors may subject themselves to individual civil or criminal prosecution for any such legal violations.

PRIVACY AND SECURITY SAFEGUARDS:

1. **I acknowledge** that I have received a copy of the Yolo County Health and Human Services Agency (HHSA) guidance entitled, *"Guidance Regarding the Confidentiality and Privacy of Information for HHSA Behavioral Health Services Employees and Contractors"* and agree to abide by all HHSA policies and procedures regarding the use and disclosure of personally identifiable information including protected health information and/or other confidential information.
2. **I understand** that in the course of my work I may learn information which is protected and/or confidential under federal and state law, or which is considered confidential and/or proprietary by HHSA. Examples include but are not limited to client health information, other personal client information, financial information, or employee information. I agree to keep confidential all such information, whether verbal, written or computerized, which I learn in the course of my work at HHSA.
3. **I understand** that I cannot discuss client or family information with anyone not immediately involved with a client's care, treatment or operations without that client's authorization. I will not discuss client or other confidential information with anyone who does not have an authorized need to know and that any discussion will be limited to the minimum necessary rules, when applicable.
4. **I understand** that confidential or proprietary information should not be discussed in areas where others may overhear such discussions (such as hallways, cubicles, elevators, etc.).
5. **I understand** that I shall not access or attempt to access any information unless the information is relevant to my job and I am authorized to access it.
6. **I understand** that any logon ID, computer password and electronic signature assigned to me by HHSA are to be used solely by me for my authorized access to information and that use of my ID and password by anyone other than me is strictly prohibited.
7. **I understand** that I am prohibited from sharing my password with anyone and I will take all necessary steps to protect the confidentiality of my login information.
8. **I understand** and agree that the use of my ID and password to use HHSA County electronic systems constitutes a digital signature and is the equivalent of my handwritten signature on the documents.

9. **I understand** that all HHSA software and hardware, including the County e-mail system and electronic health records system, are County property and subject to monitoring and review.
10. **I understand** and agree that I will only use computing devices, such as desktop computers, laptop computers, tablets, mobile phones, and external storage that are protected by HIPAA compliant encryption software, before using them for any purposes involving protected health information and/or confidential information.
11. **I understand** that I am prohibited from sending an unencrypted email if it contains protected health information and/or confidential information.
12. **I understand** that I must secure any device that contains protected health information and/or confidential information. This includes locking my desktop computer, laptop computer, tablet, mobile phone or any other device that contains access to protected health information and/or confidential information prior to leaving it unattended.
13. **I understand** and agree that I will not leave documents containing protected health information and/or confidential information in a location where persons that do not have authorization can access them. This includes:
 - Using a secure print function, if it is available;
 - Immediately retrieving documents from a printer where unauthorized persons may be able to access them, including faxes and fax confirmations;
 - placing any documents in locked cabinet when I am away from my desk.
14. **I understand** that I may be personally responsible for any breach of confidentiality resulting from an unauthorized access to data due to theft, loss, or any other compromise, as a result of me not properly securing the information.
15. **I understand** that any violation of HHSA or County policies and procedures may result in termination of contract and/or disciplinary action against me including termination of employment. Further, violation of State and federal laws also provide for civil action under the provisions of Welfare and Institutions Code Section 5330, for the greater of the following amount:
 - Ten thousand Dollars (\$10,000)
 - Three times the amount of actual damages, if any sustained by the plaintiff.
16. **I understand** and agree that this agreement shall remain in effect during my relationship with HHSA and shall continue thereafter. I agree that upon completion of contract, separation, termination or if for any other reason I am not affiliated with HHSA, I will continue to abide by the confidentiality provisions in this agreement.

//
//

17. I understand and agree that upon completion of contract or upon leaving HHSA, I will not remove any confidential or proprietary information from the County and I will return any and all confidential and/or proprietary information I may have in my possession. I have read the above confidentiality statement and I agree to comply fully with its terms.

I hereby acknowledge that I have read and understood the foregoing information and that my signature below signifies my agreement to comply with the above terms. In the event of a breach or threatened breach of the Confidentiality Statement, I acknowledge that HHSA may, as applicable and as it deems appropriate, pursue disciplinary action up to and including my termination from HHSA or the termination of my contract with HHSA.

PRINTED NAME

SIGNATURE

DATE

ORGANIZATION/JOB TITLE

EMAIL

TELEPHONE

CHECK ONE: Employee Volunteer Intern
 Temporary Employee Consultant/Contractor Other _____

For Internal Use Only:

Received By: _____

Date: _____