
 <p>Behavioral Health Department Alameda County Health</p>	<p>DocuSigned by: By:  Karyn L. Tribble, PsyD, LCSW, Director</p>
<p>POLICY TITLE</p> <p>Privacy, Security and Confidentiality Statement of Client Services, Records and Information</p>	<p>Policy No: 350-3-1</p> <p>Date of Original Approval: 10/01/2018</p> <p>Date(s) of Revision(s): 02/07/2019,^{5/10/2024}</p>

PURPOSE

To define the expectations and requirements regarding the access, use, disclosure, and the protection of client records and confidentiality of all client records created, received, maintained, or transmitted by Alameda County Behavioral Health Plan (Specialty Mental Health and Drug Medi-Cal Organized Delivery System) staff, contracted service providers, interns, volunteers, and other individuals or organizations.

AUTHORITY

- 42 Code of Federal Regulations (CFR) Part 2 Confidentiality of Alcohol and Drug Client Records
- Health Insurance Portability and Accountability Act (HIPAA)
- The Confidentiality of Medical Information Act [Civil Code Section 56 et seq.]
- Mental Health Plan (MHP) Contract
- Drug Medi-Cal Organized Delivery System (DMC-ODS) Contract

SCOPE

This policy applies to all Behavioral Health Plan (BHP) staff, contracted service providers, students, interns, volunteers, subcontractors, and any individual or organization (collectively “workforce members”) that may have access to, be provided with, and in some cases prepare and/or transmit confidential health and proprietary information. The following applies to confidential, restricted, or protected health or business information and assets that are accessed, received, or sent in any format, including digital, paper, voice, facsimile, photos, and electronic (including portable electronic devices such as, phones, laptops, USB drives).

POLICY

Workforce members with access to BHP confidential information and data systems have a legal and ethical responsibility to protect the security and confidentiality of personal, medical, financial, personnel and protected health information, and to use that information and those systems only as permitted in the performance of their jobs.

PROCEDURE

Confidential information must be treated with respect and care by any workforce member who is authorized to have access to this information. Workforce members who are authorized to use or disclose confidential information also have the responsibility to safeguard access to such information. Workforce members who are authorized by the BHP to access confidential information have a responsibility to limit access to those that are allowed by permission and/or by law. The access must be appropriate to the workforce member’s job responsibility. A breach is a violation of this policy and/or state or federal

regulatory requirements resulting in the unauthorized or inappropriate use, disclosure, or access of confidential information.

All workforce members must sign the BHP Confidentiality Statement at the time of hire and annually, thereafter. By signing this Confidentiality Statement, the workforce member hereby agrees to the following terms and conditions:

1. The workforce member will not release information to anyone concerning the financial, medical, or social status of BHP patients or clients which has not first been authorized according to written BHP policies, federal or state regulation, or otherwise properly ordered by legal authorities.
2. The workforce member will not disclose or otherwise discuss BHP patients or clients, their conditions, treatments, or status, with anyone, except to carry out assigned duties associated with their proper care of treatment. Information may only be disclosed to persons having the right to receive the information. When using or disclosing information, the workforce member will use or disclose only the minimum information necessary required to perform their assigned duties.
3. The workforce member requiring access to BHP information systems will be given a user ID and password. It is the responsibility of the workforce member to take reasonable security measures to prevent them from being lost or inappropriately acquired, modified, or otherwise compromised, and to prevent unauthorized disclosure of, access to, or use of them, or of any media on which information about them (i.e., login credentials) are stored. The workforce member will not, at any time or under any circumstances, share or disclose any assigned computer system user Identification or password to anyone. If the workforce member suspects their user ID or password has been stolen or inappropriately acquired, lost, used by an unauthorized party, or otherwise compromised, the workforce member will immediately notify the appropriate Information Systems (IS) Help Desk and submit a privacy incident report.
4. The workforce will not tamper with any BHP's computer system to gain unauthorized access to the network or information contained therein. The hardware, software, data and outputs of BHP information systems are the property of the BHP and must be appropriately licensed for installation on any BHP issued computer or devices.
5. The workforce member will take all reasonable care to prevent the unauthorized use, disclosure, or availability of confidential and/or proprietary information through unattended screen displays or by mishandling of system generated output, regardless of its form.
6. The workforce member will not download or maintain patient or client information on privately-owned computer, laptop, or other portable devices.
7. The workforce member acknowledges that all records, files, or other objects maintained by or under the control, custody, or possession of BHP, including, without limitation, paper, or electronic medical records, shall be and remain the property of BHP. Upon termination of the working relationship, the workforce member shall return all such property received from BHP within five (5) business days. BHP strictly prohibits traveling with County-issued or owned

portable electronic devices (e.g., laptops, tablets, mobile phones) outside of the USA. Moreover, accessing confidential patient or client information while outside the USA is strictly prohibited. The ACH Chief Compliance and Privacy Officer and IS Director must expressly approve and document all exceptions to this policy.

8. The workforce member understands and acknowledges that BHP retains the right to monitor and/or review, at any time and without cause, any access to BHP’s computer, network, or information systems for evidence of tampering or misuse, and may, at its sole discretion, suspend or terminate the workforce member’s privileges pending administrative review. In addition, any misconduct and/or breaches of confidentiality expressly described herein may be grounds for immediate suspension of privileges and may result in termination of employment or contract. Unauthorized use or disclosure of confidential information may be subject to civil and criminal penalties under provisions of federal and state regulations.

NON-COMPLIANCE

Non-compliance with this policy, Confidentiality Statement, or any federal or state privacy and confidentiality laws may result in suspension of privileges, or termination of employment or contract. All known violations of this policy, including privacy or security incidents and breaches, must be reported through the [Privacy Incident Reporting](#) form within 24-hours of discovery. Questions or concerns regarding suspected violations of this policy can be submitted either via email to breachnotification@acgov.org, or via completion of the [Privacy Incident Reporting](#) form within 24-hours of discovery.

CONTACT

ACBH Office	Current Date	Email/Phone
Quality Assurance (QA)	5/9/2024	QAOffice@acgov.org
Office of Compliance Services	5/9/2024	HCSA.Compliance@acgov.org

DISTRIBUTION

This policy will be distributed to the following:

- ACBHD Staff
- ACBHD County and Contracted Providers
- Public

ISSUANCE AND REVISION HISTORY

Original Authors: Sharon Loveseth, LAADC, HSE, SUD Program Specialist, QA

Original Date of Approval: 10/01/2018 by Carol F. Burton, MSW, Interim Behavioral Health Director

Revision Author	Reason for Revision	Date of Approval by (Name, Title)
Sharon Loveseth, LAADC, HSE; SUD Program Specialist, QA	Monitoring and Technical Improvements	02/07/2019 by Rudy Arrieta
Ravi Mehta, Chief Compliance and Privacy Officer	Alignment with current ACBHD policies and updating of outdated language.	5/10/2024 by Karyn L. Tribble, PsyD, LCSW, Behavioral Health Director

DEFINITIONS

Term	Definition
Patient	Refers to clients, beneficiaries, consumers, persons served, and patients

APPENDICES

Confidentiality Statement ACBH Form (Note: Internal County staff can access the form at eforms3.bhcs.internal/lincdoc/doc/run/alameda/Oath_Confidentiality, while contracted service providers must log in to Citrix and access the E-Forms app where they will find the form “Confidentiality Statement.”)