Alameda Family Services

2325 clement avenue, suite a
alameda ca 94501

DATE: April 23, 2015

SUBJECT: Privacy and Confidentiality

1. To protect the privacy of agency clients
2. To comply with applicable laws and regulations.
3. To insure fair information practices as to:
    a. Openness
    b. Accountability
    c. Collection limitations
    d. Purpose and use limitations
    e. Access and correction
    f. Data Quality
    g. Security

STATEMENT OF POLICY:

1) Alameda Family Services privacy practices will comply with all applicable laws governing HMIS client privacy/confidentiality. Applicable standards include, but are not limited to the following.
    a) Federal Register Vol. *69. No. 146 (I IMIS* FR *4848-N-02)* - Federal statute governing HMIS information – Friday, July 30, 2004.
    b) HIPAA - the Health Insurance Portability Act.
    c) 42 CFR Part 2. - Federal statute governing drug and alcohol treatment (attached as Appendix A)
    d) Alameda County-wide Continuum of Care InHOUSE Policy and Procedures manual.
    e) Alameda County-wide Continuum of Care InHOUSE partner agency sharing agreement(s).

2) **Use of Information** PPI (protected personal information which can be used to identify a specific client) can be used only for the following purposes:
    a) To provide or coordinate services to a client.
    b) For functions related to payment or reimbursement for services.

c) To carry out administrative functions such as legal, audit, personnel planning, oversight and management functions.

d) For creating de-personalized client identification for unduplicated counting.

e) Where disclosure is required by law.

f) To prevent or lessen a serious and imminent threat to the health or safety of an individual or the public.

g) To report abuse, neglect, or domestic violence as required or allowed by law.

h) Contractual research where privacy conditions are met (including a written agreement).

i) To report criminal activity on agency premises.

j) For law enforcement purposes in response to a properly authorized request for information from a properly authorized source.

3) **Collection and Notification** Information will be collected only by fair and lawful means with the knowledge or consent of the client.

a) PPI will be collected only for the purposes listed above, and entered into InHOUSE.

b) Clients will be made aware that personal information is being collected and recorded and will be asked to express written consent to have their basic intake information shared in the InHOUSE system.

c) A written sign will be posted in locations where PPI is collected. This written notice will read:

> "*We collect personal information directly from you for reasons that are discussed in our Privacy Notice. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate.*
>
> *The collection and use of all personal information is guided by strict standards of confidentiality. Our Privacy Notice is posted. A copy of our Privacy Notice is available to all clients upon request."*

d) This sign will be explained in cases where the client is unable to read and/or understand it.

4) **Data Quality** PPI data will be accurate, complete, timely, and relevant.

a) All PPI collected will be relevant to the purposes for which it is to be used.

b) Identifiers will be removed from data that is not in current use after 7 years (from date of creation or last edit) unless other requirements mandate longer retention.

c) Data will be entered in a consistent manner by authorized users.

d) Data will be entered in as close to real-time data entry as possible.

e) Measures will be developed to monitor data for accuracy and completeness and for the correction of errors.

   i) The agency runs reports and queries monthly to help identify incomplete or inaccurate information.

   ii) The agency monitors the correction of incomplete or inaccurate information.

   iii) By the 15th of the following month all monitoring reports will reflect corrected data.

f) Data quality is subject to routine audit by System Administrators who have administrative responsibilities for the database.

5) **Privacy Notice, Purpose Specification and Use Limitations** The purposes for collecting PPI data, as well as it uses and disclosures will be specified and limited.

a) The purposes, uses, disclosures, policies, and practices relative to PPI data are to be outlined in this agency Privacy Notice.

b) The agency Privacy Notice will comply with all applicable regulatory and contractual limitations.

c) The agency Privacy Notice will be made available to agency clients, or their representative, upon request and explained/interpreted as needed.

d) Reasonable accommodations will be made with regards to the Privacy Notice for persons with disabilities and non-English speaking clients as required by law.

e) PPI will be used and disclosed only as specified in the Privacy Notice, and only for the purposes specified therein.

f) Uses and disclosures not specified in the Privacy Notice can be made only with the consent of the client.

g) The Privacy Notice will be posted on the agency web site.

h) The Privacy Notice will reviewed and amended as needed.

i) Amendments to or revisions of the Privacy Notice will address the retroactivity of any changes.

j) Permanent documentation will be maintained of all Privacy Notice amendments/revisions.

k) All access to, and editing of PPI data will be tracked by an automated audit trail, and will be monitored for violations use/disclosure limitations.

6) **Record Access and Correction** Provisions will be maintained for the access to and corrections of PPI records.

a) Clients will be allowed to review their InHOUSE record within 5 working days of a request to do so.

b) During a client review of their record, an agency staff person must be available to explain any entries the client does not understand.

c) The client may request to have their record corrected so that information is up-to-date and accurate to ensure fairness in its use.

d) When a correction is requested by a client, the request will be documented and the staff will make a corrective entry if the request is valid.

e) A client may be denied access to their personal information for the following reasons:

   i) Information is compiled in reasonable anticipation of litigation or comparable proceedings;

   ii) Information about another individual other than the agency staff would be disclosed,

   iii) Information was obtained under a promise of confidentiality other than a promise from this provider and disclosure would reveal the source of the information

   iv) The disclosure of information which would be reasonably likely to endanger the life or physical safety of any individual.

f) A client may be denied access to their personal information in the case of repeated or harassing requests for access or correction. However, if denied, documentation will be provided regarding the request and reason for denial to the individual and be made a part of the client's record.

g) A grievance process may be initiated if a client feels that their confidentiality rights have been violated, if access has been denied to their personal records, or if they have been put at personal risk, or harmed.

h) Any client grievances relative to the InHOUSE system will be processed/resolved according to agency grievance policy.

i) A copy of any client grievances relative to InHOUSE data or other privacy/ confidentiality issues and agency response are forwarded to CoC staff.

j) If a client is unsatisfied with the resolution of their grievance at the agency level, the client may request mediation at the system level.

7) **Accountability**: Processes will be maintained to insure that the privacy and confidentiality of client information is protected and staff is properly prepared and accountable to carry out agency policies and procedure that govern the use of PPI data.

a) Grievances may be initiated through the agency grievance process for considering

questions or complaints regarding privacy and security policies and practices. All users of the InHOUSE system must sign a Users Agreement that specifies each staff persons' obligations with regard to protecting the privacy of PPI and indicates that they have received a copy of the agency's Privacy Notice and that they will comply with its guidelines.

b) All staff, interns, volunteers or associates collecting PPI intended for, or viewing data generated by InHOUSE must successfully complete Council-sponsored privacy and security certification training.

c) A process will be maintained to document and verify completion of training requirements.

d) A process will be maintained to monitor and audit compliance with basic privacy requirements including but not limited to auditing clients entered against signed InHOUSE Consent Releases. At minimum, a quarterly Compliance Review will be conducted and documented.

e) A copy of any staff grievances initiated relative to privacy, confidentiality, or InHOUSE system data will be forwarded to CoC Staff.

f) Regular user meetings will be held and issues concerning data security, client confidentiality, and information privacy will be discussed and solutions will be developed.

8) **Sharing of Information:** Basic Intake data may be shared with partnering agencies only with client approval

a) All routine data sharing practices with partnering agencies will be documented and governed by the CoC MOU Agreement that defines the agency-determined sharing practice.

b) Resident name and social security number are viewable in InHOUSE without express written consent for the purpose of searching for a client in the software. Procedures are available to not enter name and/or social security number from the searchable field.

c) A completed InHOUSE Client Release of Information (ROI) Form is needed before information may be shared electronically.

i) The InHOUSE release is to inform the client about what is shared and with whom it is shared.

ii) The client accepts or rejects the sharing plan.

iii) Revisions to the consent for sharing the Basic intake may be requested by the resident during the standard business hours. Changes will not be retroactive.

d) Clients will be informed about and understand the benefits, risks, and available alternatives to sharing their information prior to signing an ROI, and their decision to grant permission shall be voluntary.

e) Clients who choose not to authorize sharing of information cannot be denied services for which they would otherwise be eligible.

f) All Client Authorization for ROI forms related to the InHOUSE system will be placed in a file to be located on premises and will be made available to the CoC Staff for periodic audits.

g) InHOUSE-related Authorization for ROI forms will be retained for a minimum period of three (3) years, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised.

h) No confidential/restricted information received from the InHOUSE system will be shared with any organization or individual without proper written consent by the client, unless otherwise permitted by applicable regulations or laws.

i) Restricted information, including progress notes and psychotherapy notes about the diagnosis, treatment, or referrals related to a medical health, disabilities, mental health disorder, drug or alcohol use, HIV/AIDS, and any violence-related concerns shall <u>not</u> be shared with other participating Agencies without the clients written, informed consent as documented on the Agency Authorization for Release of Restricted Information Form.

   i) Sharing of restricted information is <u>not</u> covered under the general InHOUSE Client ROI.

   ii) Sharing of restricted information must also be planned and documented through a fully executed Authorization for Release of Restricted Information Form

j) If a client has previously given permission to share information and then chooses to revoke that permission by completing a new ROI, the InHOUSE Basic Intake will be closed to further sharing.

k) All client ROI forms will include an expiration date, and once a Client ROI expires, any new information entered will be closed to sharing unless a new Client ROI is signed by the client and entered in the InHOUSE system.

9) **<u>System Security</u>:** System security provisions will apply to all systems where PPI is stored: agency's networks, desktops, laptops, mini-computers, mainframes and servers.

a) Password Access:

   i) Only individuals who have completed Privacy and Security Certification and Software Training may be given access to the InHOUSE system through User IDs and Passwords,

   ii) Temporary default passwords will be changed on first use.

   iii) Access to PPI requires a user name and password at least 8 characters long and using at least one number and one letter.

   iv) Passwords will not use or include the users name or the vendor name, and will not consist entirely of any word found in the common dictionary or any of the above words spelled backwards.

v) User Name and password may not be stored or displayed in any publicly accessible location.

vi) Passwords must be changed routinely.

vii) Users must not be able to log onto more than one workstation or location at a time.

viii) Individuals with User IDs and Passwords will not give or share assigned User IDs and Passwords to access the InHOUSE system with any other person, organization, governmental entity, business.

b) Virus Protection and Firewalls:

i) Commercial anti-virus protection software will maintained to protect all agency network systems and workstations from virus attack.

ii) Virus protection will include automated scanning of files as they are accessed by users.

iii) Virus Definitions will be updated regularly.

iv) All workstations will be protected by a firewall either through a workstation firewall or a server firewall.

c) Physical Access to Systems where InHOUSE Data is Stored

i) Computers stationed in public places must be secured when workstations are not in use and staff is not present.

ii) After a short period of time a pass word protected screen saver will be activated during time that the system is temporarily not in use.

iii) For extended absence from a workstation, staff must log off the computer.

d) Stored Data Security and Disposal:

i) All InHOUSE data downloaded onto a data storage medium must be maintained and stored in a secure location, not accessible to non-licensed users of the InHOUSE system.

ii) Data containing PPI will not be downloaded to any remote access site at any time for any reason, nor transmitted outside the physical agency by any means whatsoever.

iii) Data stored on a portable medium will be secured when not in use and will never be taken off site at any time for any reason.

iv) Data downloaded for purposes of statistical analysis will exclude PPI whenever possible.

v) InHOUSE data downloaded onto a data storage medium must be disposed of by reformatting as opposed to erasing or deleting. This includes hard drives.

vi) A data storage medium will be reformatted a second time before the medium is reused or disposed of.

e) System Monitoring

i) User access to the InHOUSE Live Web Site will be monitored using the computer access logs located on each computer's explorer "history" button, or via a central

server report.

f) Hard Copy Security:

i) Any paper or other hard copy containing PPI that is either generated by or for InHOUSE including, but not limited to report, data entry forms and signed consent forms will be secured.

ii) Agency staff will supervise at all time hard copy with identifying information generated by or for the InHOUSE system when the hard copy is in a public area. If the staff leaves the area, the hard copy must be secured in areas not accessible by the public.

iii) All written information pertaining to the user name and password must not be stored or displayed in any public accessible location.

g) Authorized Location Access:

i) Access to the InHOUSE system is allowed only from authorized agency locations.

10) **Agency HMIS/InHOUSE Grievance Policy: See Appendix B**

APPENDIX A

Privacy, 42CFR

The Provider List is a list of contracted providers of mental health and substance use disorder services in our community. The County ACCESS program makes referrals for all outpatient non-emergency services. You may contact ACCESS at 1-800-491-9099 for further information regarding the Provider List, including whether a provider has current openings.

Confidentiality and Privacy

The confidentiality and privacy of what you discuss at this service site is an important personal right of yours. This packet contains your copy of the "Notice of Privacy Practices" document, which explains how your records and personal information are kept confidential.

In certain situations involving your safety or the safety of others, providers are required by law to discuss your case with people outside the Behavioral Health Care system.

Those situations include:

1. If you threaten to harm another person(s), that person(s) and/or the police must be informed.
2. When necessary, if you pose a serious threat to your own health and safety.
3. All instances of suspected child abuse must be reported.
4. All instances of suspected abuse of an elder/dependant adult must be reported.
5. If a court orders us to release your records, we must do so.

If you have any questions about these limits of confidentiality, please speak with the person explaining these materials to you. More information about the above and other limits of confidentiality is in the "Notice of Privacy Practices" section of this packet.

Many of the Substance Use Disorder (SUD) services provided through Alameda BHS programs are funded through the federal Medicaid Program and is administered by the state as the California Medical Assistance Program (Medi-Cal).

Advance Directive Information:

"Your Right to Make Decisions about Medical Treatment"

(Only applies if you are age 18 or older)

Providers: "Your Right to Make Decisions about Medical Treatment," is available in English at http://www.acbhcs.org/providers/QA/docs/qa_manual/10-7_ADVANCE_DIRECTIVE_BOOKLET.pdf, n the QA tab. The same information, in the five threshold languages, is also online in booklet format.

If you are age 18 or older, the Mental Health Plan is required by federal & state law to inform you of your right to make health care decisions and how you can plan now for your medical care,

in case you are unable to speak for yourself in the future. Making that plan now can help make sure that your personal wishes and preferences are communicated to the people who need to know. That process is called creating an Advance Directive.

You can access the booklet about Advance Directives called, "Your Right to Make Decisions about Medical Treatment" by going to the link listed above. It describes the importance of creating an Advance Directive, what kinds of things you might consider if you decide to create one, and it describes the relevant state laws. You are not required to create an Advance Directive but we do encourage you to explore and address issues related to creating one. Alameda County BHCS providers and staff are able to support you in this process, but are not able to create an Advance Directive for you. We hope the information will help you understand how to increase your control over your medical treatment.

The care provided to you by any Alameda County BHCS provider will not be based on whether you have created an Advance Directive. If you have any complaints about Advance Directive requirements, please contact the California Department of Health Services Licensing and Certification by calling 1-800-236-9747 or by mail at P.O. Box 997413, Sacramento, CA 95899-7413.

Your Right to Vote

Register to Vote Now

You can apply to register to vote right now by filling in the online application. To register to vote in California you must be A United States Citizen, A resident of California, and 18 years of age or older. If you have any questions, call 510-272-6973 or visit Frequently Asked Questions, on-line at https://www.acgov.org/alco_ssl_app/rov/voter_info/voter_profile.jsp?formLanguage=E

THIS NOTICE DESCRIBES HOW MEDICAL & DRUG & ALCOHOL RELATED INFORMATION ABOUT YOU MAY BE USED & DISCLOSED & HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

42 CFR, Part 2: General information regarding your health care, including payment for health care, is protected by two federal laws: the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1320d et seq., 45 C.F.R. Parts 160 & 164, & the Confidentiality Law, 42 U.S.C. § 290dd-2, 42 C.F.R. Part 2. Under these laws, your Substance Use Disorder ("SUD") Treatment Provider may not say to a person outside of the program that you attend the program, nor may the Provider disclose any information identifying you as an alcohol or drug treatment patient, or disclose any other protected information except as permitted by federal law.

A Provider must obtain your written consent before it can disclose information about you for payment purposes. For example, the Provider must obtain your written consent before it can disclose information to your health insurer in order to be paid for services. The Provider is also required to obtain your written consent before it can sell information about you or disclose information about you for marketing purposes, and the Provider must obtain your written consent before disclosing any of your psychotherapy records. Generally, you must also sign a written consent before the Provider can share information for treatment purposes or for health care operations. However, federal law permits the Provider to disclose information *without* your written permission:

1. Pursuant to an agreement with a qualified service organization/business associate;
2. For research, audit or evaluations;
3. To report a crime committed on the Provider premises or against Provider personnel;
4. To medical personnel in a medical emergency;
5. To appropriate authorities to report suspected child abuse or neglect;
6. As allowed by a court order.

Before the Provider can use or disclose any information about your health in a manner which is not described above, it must first obtain your specific written consent allowing it to make the disclosure. Any such written consent may be revoked by you orally or in writing.

Your Rights Under HIPAA, you have the right to request restrictions on certain uses & disclosures of your health information. The Provider is only required to agree to your request if you request a restriction on disclosure to your health plan for payment or health care operations purposes, and you pay for the services you receive from the Provider yourself (out-of-pocket), unless the disclosure is otherwise required by law. In any other situation, the Provider is not required to agree to any restrictions you request, but if it does agree then it is bound by the agreement and may not use or disclose any information which you have restricted except as necessary in a medical emergency.

You have the right to request that we communicate with you by alternative means or at an alternative location. The Provider will accommodate such requests that are reasonable & will not request an explanation from you. Under HIPAA you also have the right to inspect & copy your own health information maintained by the Provider including electronic a copy, except to the extent that the information contains psychotherapy notes or information compiled for use in a civil, criminal or administrative proceeding or in other limited circumstances.

Under HIPAA you also have the right, with some exceptions, to amend health care information maintained in the Provider records, and to request and receive an accounting of disclosure of your health related information made by the Provider during the six years prior to your request. You also have the right to receive this notice.

Provider Duties The Provider is required by law to maintain the privacy of your health information and to provide you with notice of its legal duties and privacy practices with respect to your health information. The Provider is required by law to abide by the terms of this notice and to make new notice provisions effective for all protected health information it maintains. Revision and update notices will be provided to individuals during treatment sessions and will be posted on the Public Notice Board in the

lobby.

Complaints and Reporting Violations You may complain to the Provider and the Secretary of the United States Department of Health and Human Services if you believe that your privacy rights have been violated under HIPAA. (See HIPAA Privacy Notice for complaint procedures). Violation of the Confidentiality Law by a program is a crime. Suspected violations of the Confidentiality law may be reported to the United States Attorney in the District where the violation occurs.

For further information, contact Alameda County BHCS Access Unit at: **1-800-491-9099**

NOTICE OF PRIVACY PRACTICES

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. PLEASE REVIEW IT CAREFULLY.

Your Rights

Get a copy of your health and claims records:

- You can ask to see or get a copy of your health and claims records and other health information we have about you.
- We will provide a copy or a summary of your health and claims records, usually within 30 days of your request. We may charge a reasonable, cost –based fee.

Ask us to correct health and claims records:

- You can ask us to correct your health and claims records if you think they are incorrect or incomplete.
- We may say "no" to your request, but we'll tell you why in writing within 60 days...

Request confidential communications

- You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address.
- We will consider all reasonable requests, and must say "yes" if you tell us you would be in danger if we do not

Ask us to limit what we use or share

- You can ask for a list of the times we've shared your health information for six years prior to the date you ask, whom we shared it with and why.
- We are not required to agree to your request, and we may say "no" if it would affect your care.

Get a copy of the privacy notice.

- You can ask for a paper copy of this notice at any time, even if you have agreed to receive this notice electronically. We will provide you with a copy promptly.

Choose someone to act for you.

- If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information.

situation described below, talk to us. Tell us what you want us to do, and we will follow your instructions.

- Share information with your family, close friends, or others involved in payment for your care.
- Share information in a disaster relief situation
- Contact you for fundraising efforts

If you are not able to tell us your preference, for example fi you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.

In these cases, marketing purposes or sale of your information, we never share your information unless you give us permission.

Our Uses and Disclosures

- Medical Treatment: information for payment, your medical care, leave an appointment reminder messages with your permission, to tell you about services or treatment, business associates, labs, pharmacies, and interpreters.
- Special Situations: to talk to people who help pay for your care, workers compensation, to schedule an interpreter for you in the event of a disaster, to prevent or control disease, to report births or deaths, healthcare emergency, eminent threat to self or others.
- Legal Purposes: for specific court requests such as subpoenas, to report suspected abuse, neglect or domestic violence, for investigations for audits, to jails or prisons, for national security or to protect the President.

Our Responsibilities

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach

- We will make sure the person ahs this authority and can act for you before we take any action.

File a complaint if you feel your rights are violated.

- You can complain if you feel we have violated your rights by contacting us.
- You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Ave. S.W., Washington, D.C., 20201; 1-877-696-6775 or visiting: www.hhs.gov/ocr/privacy/hipaa/complaints/.
- We will not retaliate against you for filing a complaint.

Your Choices

For certain health information, you can tell us your choices about what we share. If you have a clear preference for how we share your information in the

occurs that may have compromised the privacy or security of your information.

- We must follow the duties and privacy practices described in this notice and give you a copy.
- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

Changes to the Terms of this Notice: We can change the terms of this notice, and the changes will apply to all information we have about. The new notice will be available upon requires, on our website, and we will mail a copy to you.

For More Information & A Copy in Other Languages: DHCS Privacy officer:866-866-0602 #1; TTY 877-735-2929
Email: privacyofficer@dhcs.ca.gov
Mail to: P.O. Box 997413 MS4721, Sacramento,CA 95899-7413

APPENDIX B: DREAMCATCHER YOUTH SERVICES

CLIENT GRIEVANCE POLICY

WHAT TO DO IF YOU HAVE A GRIEVANCE

If you have a complaint about the performance of DreamCatcher Youth Services staff, and/or you feel you have been treated unfairly, the following are the steps you should take to have your complaint heard:

1. Talk privately to the person with whom you have the problem. We encourage you to try first to work out the problem in an open and informal way.

2. If you do not feel comfortable talking with the person with whom you have the problem, or you do talk with them and are not satisfied with the outcome, you may make an appointment to speak with or submit a written complaint (which may be in your own language) to the DreamCatcher Youth Services Director. If you have good cause to use another medium to communicate your complaint, such as a tape recording, you may do so. The Director shall meet with you or provide you with a written response to your written complaint within ten (10) working days of the meeting or receipt of your written complaint.

3. Or, if you prefer, you may bypass the above steps and immediately contact the funding agency below:

Alameda county Social Services Agency Administrative Offices
2000 San Pablo Avenue, 4th Floor, Oakland CA 94612

ATT: Lori A. Cox, Social Services Agency Director
(510)-271-9100

I certify that the information in this document was explained to my satisfaction in my own language and a copy of this form was given to me.

_____

Client's Name (printed)

_____

Client's Signature Date