

PRIVACY POLICY

DATE: September 9, 2005
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) Compliance Agency 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 (*1 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.
 - 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 that is 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.
 - 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 information entered 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 its 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 be 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) Information, the disclosure of 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 users of the InHOUSE system must complete formal privacy 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** Client 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) 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, and selects the extent of sharing.
 - iii) If the client rejects the sharing plan, staff will click the Security Button, which closes the record.
 - iv) If the client selects collaborative sharing only, the record is "closed" with designated exceptions.
 - c) 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.
 - d) Clients who choose not to authorize sharing of information cannot be denied services for which they would otherwise be eligible.
 - e) 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.
 - f) 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.
 - g) 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.

- h) 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 not 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 not 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
 - iii) If a field that normally contains non-confidential information discloses confidential information.
 - (1) The staff completes an Authorization for Release of Restricted Information Form.
 - (2) If the client refuses to authorize the release, the staff closes the Assessment/Screen by clicking the lock on the screen and removing any exceptions.
 - i) If a client has previously given permission to share information with multiple agencies, beyond basic identifying information and non-restricted service transactions, and then chooses to revoke that permission with regard to one or more of these agencies, the affected agency/ agencies will be contacted accordingly, and those portions of the record impacted by the revocation, too will be locked from further sharing.
 - j) 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) **System Security** 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 System 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.
 - iii) InHOUSE data downloaded onto a data storage medium must be disposed of by reformatting as opposed to erasing or deleting. This includes hard drives.
 - iv) 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

1. **GRIEVANCE PROCEDURES:** If a client has a disagreement with his/her Case Manager, or with a resident advisor, s/he can:
 - Request to speak to the Case Manager's supervisor, including the Shelter Coordinator and/or Assistant Shelter Coordinator.
 - If not satisfied after speaking with the supervisor, s/he can request to speak to the Program Director for Covenant House Oakland.
 - If I am still not satisfied, I can file a formal grievance, either verbally or in writing, to the Associate Executive Director (AED). The AED can be reached by asking any staff person to contact her at her phone extension (249), or I can set up an appointment with her assistant at her extension (253).
 - The AED will interview the resident regarding his/her grievance in a confidential, onsite office. If the client is no longer in the residential program and requires transportation to the CHC facility, transportation will be provided by CHC.
 - Within 72 hours of receiving the grievance, the AED will gather information, facts and testimony from residents and staff relevant to the complaint and present the resolution to the client in both written and verbal form.

- If the client is dissatisfied with the grievance resolution proposed by the AED, s/he will be provided – in writing – with the name, address and phone of an outside resolution service: