MARIN COUNTY CONTINUUM OF CARE

HOMELESS MANAGEMENT INFORMATION SYSTEM

PRIVACY NOTICE

PURPOSE:

The purpose of this Notice is to advise agency employees of the HMIS legal requirements to;

a) protect the privacy of agency clients
b) comply with applicable laws and regulations
c) insure fair information practices relating to:
    i. Openness
    ii. Accountability
    iii. Information collection limitations
    iv. Purpose and use limitations
    v. Access to and correction of information
    vi. Data quality
    vii. Security

PRIVACY - STATEMENT OF POLICY:

1) Marin County Continuum of Care privacy practices will comply with all applicable laws governing Homeless Management Information System (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 and Accountability Act.

    c) 42 CFR Part 2. - Federal statute governing confidentiality of Substance Use Disorder treatment records.

    d) Marin County Continuum of Care policies and procedures.

    e) Marin County Continuum of Care Governance Charter.

2) **Use or disclosure of Confidential Information:** (which includes but is not limited to protected personal information (PPI), 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 HMIS.

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 HMIS 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 to clients where the client is unable to read and/or understand it.

4) **Data Quality:** 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 3 years (from last service) 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.

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 outlined in this Privacy Notice.

b) This agency Privacy Notice complies with all applicable regulatory and contractual limitations.

c) This agency Privacy Notice is available to agency clients, or their representative, upon request and explained/interpreted as needed.

d) Reasonable accommodations will be made with regards to this 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, if there is an agency website.

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

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

j) Privacy Notice amendments/revisions will be maintained for 6 years following the amendment or revision.

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

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

a) Clients will be allowed to review their HMIS 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 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 HMIS system will be processed/resolved according to agency grievance policy.

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

7) **Accountability:** Processes will be maintained to insure that the privacy and confidentiality of client information is protected and that agency staff are properly prepared and accountable to carry out agency policies and procedures 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 HMIS system must sign a User Agreement that specifies each staff persons' obligations with regard to protecting the privacy of PPI and indicates that they have received a copy of this 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 HMIS must successfully complete privacy and security 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 HMIS Authorization to Release PPI. At minimum, an annual Compliance Review will be conducted and documented.

e) 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 Continuum of Care Agreement that defines the sharing practices.

b) A completed HMIS client Release of Information (ROI) Form is needed before information may be shared electronically.

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

ii) The client accepts or rejects the sharing plan.

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 ROI forms related to the HMIS system will be retained in an easily retrievable format and system whereby the Continuum of Care Staff may periodically review and audit them.

f) HMIS related ROI forms will be retained for a minimum period of three (3) years, after the last service has been provided to the client. After the retention period the forms will be destroyed in a manner that ensures client confidentiality is not compromised.

g) No confidential/restricted information received from the HMIS 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 about the diagnosis, treatment, or referrals related to medical health, disabilities, mental health disorder, substance use, HIV/AIDS, and any violence-related concerns shall not be shared with other participating Agencies without the client's written informed consent as documented on the Agency Authorization for Release of Information Form.

i) Sharing of restricted information is not covered under the general HMIS client ROI.

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

i) If a client has previously given permission to share information and then chooses to revoke that permission in writing, the HMIS Basic Intake will be closed to 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 HMIS 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 Security Training may be given access to the HMIS 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 consistent with the Continuum of Care policy and procedures.

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

v) Passwords must be changed in accordance with the Continuum of Care policy and procedures.

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

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

b) Virus Protection and Firewalls:

i) Commercial anti-virus protection software will be 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 HMIS 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 HMIS data downloaded onto a data storage medium must be maintained and stored in a secure location, not accessible to non-approved or unauthorized users of the HMIS system.

ii) Data containing Confidential Information (including PPI) will not be downloaded to any remote access site at any time for any reason, nor transmitted outside the physical agency without using e-mail encryption that meets current industry standards (128 bit encryption).

iii) Data stored on a portable medium will be secured when not in use and will never be taken off site at any time without approval from the Continuum of Care.

iv) Data downloaded for purposes of statistical analysis will exclude personally identifiable information, including PPI, unless specific purposes have been approved by the Continuum of Care.

v) HMIS 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 HMIS will be monitored using a central server report.

f) Hard Copy Security:

i) Any paper or other hard copy containing Confidential Information, including PPI, that is either generated by or created for HMIS, including but not limited to reports, data entry forms and signed consent forms will be secured from unauthorized access.

ii) Agency staff will supervise hard copy, with personally identifying information, generated by or created for the HMIS system, when the hard copy is in a public area. If the staff leave the area, the hard copy must be secured in areas not accessible by the public.

g) Authorized Location Access:

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

10) **Agency HMIS Grievance Policy**: The purpose of the Grievance Policy is to allow clients to express concerns and have correction implemented. Clients will contact the Participating Agency with which they have an HMIS data related grievance for resolution of problems.

Participating Agencies will follow the grievance process outlined in the Continuum of Care Policy and Procedures.