CBHS Policies and Procedures

City and County of San Francisco
Department of Public Health
Community Programs
COMMUNITY BEHAVIORAL HEALTH SERVICES

1380 Howard Street, 5th Floor
San Francisco, CA 94103
415.255-3400
FAX 415.255-3567

POLICY/PROCEDURE REGARDING: **Behavioral Health Information Systems Access Control Policy**

Issued By: Jo Robinson, MFT
Director of Community Behavioral Health Services

Date: January 25, 2011

Manual Number: 6.00-06
References:

New Policy

Purpose:

To establish policies and provide guidelines related to obtaining, creating, maintaining, and closing Behavioral Health information systems user access accounts. To operationalize information system user access security and privacy policies of the San Francisco Department of Public Health (SFDPH.) These policies and guidelines are specifically intended to respond to the SFDPH Information Systems Security Policy: "Access Control". Further, to insure the utmost security and safety for client records, this policy and CBHS administrative, physical and electronic recordkeeping practices adhere to Code of Federal Regulations 45, part 164.

Scope:

This policy applies to all programs and personnel; including permanent, temporary, intern, volunteer, and contract personnel that utilize Behavioral Health Services (BHS) information systems. This policy applies to all networks; computing devices; and related data, equipment, and software owned or operated by BHIS and used for the purpose of recording, documenting, processing or transmitting client and other health care related data; including but not limited to, billing, authorizations, claiming, clinical, provider management, and other related information utilized by the Departments of Community Behavioral Health Services, CBHS).

CBHS provides the following services to BHIS users:

Avatar Suite licenses and Subscriptions

Includes RADPlus, Cache, Java, Infoscriber

Token, VPN or direct LAN/WAN connectivity

Avatar Install disks and installation consultation and support

Full service installation and configuration to Civil Service programs

Consultation support to contract organizations.

eMail accounts to Civil Service programs and employees

Includes eMail to contract employees reporting directly to a Civil Service Supervisor or program only.

Internet access to Civil Service programs

Contract programs are responsible for providing broadband internet access for Avatar users

1. Policy

1.1. Authorization

1.1.1. Access to Behavioral Health information systems requires

1.1.1.1. Written authorization by a director, supervisor, or manager designated by the Department of Public Health (DPH) or Community Behavioral Health Services (CBHS).

1.1.1.2. Signed employee oath of confidentiality and attestation of policy awareness and acceptance.

1.1.2. Levels of access and permissions assigned to a user are based on the "need to know" and on the access required to accomplish assigned job duties and responsibilities.

1.1.3. Each user is identified by a unique logon name authenticated by a user set password. Logon and password is consistent with the current version of the DPH Information System Security Policy: "Password Policy."

1.1.3.1. User login and password provide electronic signature as defined in the CBHS Electronic Signature Policy # 6.00-01

1.1.4. Access to BHIS is inactivated upon notice that a user has had privileges suspended or revoked by the CBHS Compliance Unit, been terminated or transferred or no longer requires access due to changes in job description or functions.

1.1.4.1. CBHS Compliance Unit is responsible for notifying BHIS immediately upon suspension or termination of staff privileges.

1.1.4.2. Supervisors are responsible for notifying BHIS within 5 working days when a user is terminated or transferred or no longer requires access due to changes in job description or duties.

1.1.4.3. Supervisors are responsible for notifying BHIS prior to, or immediately upon termination of a user from employment as the result of disciplinary action.

1.2. Training

1.2.1. Access to any DPH network or information system requires training in system security and Departmental policies related to security, confidentiality and privacy, use of email, use of the World Wide Web, use of Department resources to conduct personal business, general use of electronic computing resources, and other policies that may apply to specific programs or systems.

1.2.2. Access to Behavioral Health Information Systems (BHIS) requires training related to maintenance of data integrity, confidentiality of protected health information (PHI); rules and regulations related to information system security; ownership, privacy, and confidentiality of electronic records; compliance with program specific policies and

regulations for data maintenance and integrity, and proficiency in use of related data systems and computer applications.

1.2.3. Access to the CHC Data warehouse system and other data stores requires additional training in security, confidentiality of electronic records, and rules and regulations related to use of healthcare related data for research, planning or evaluation.

1.2.4. Remote access to any DPH network and CBHS information system requires declaration of need for such access and authorization by a supervisor. (See SFDPH Information Systems Security Policy: "Remote Network Access")

1.2.5. Training to this policy is required at initiation of account, during yearly updates, and when this policy is updated or changed.

1.2.6. BHIS training, proficiency in use of computer applications, and review of and adherence to information system policies are incorporated into BHS employee orientation, training curricula, and performance appraisal systems.

1.2.7. BHIS provides training and certification for on-site program trainers upon request of program supervisor of director.

1.2.8. BHIS provides oversight of information system training quality.

1.3. Creation and Maintenance of User Accounts

1.3.1. Responsibility for user accounts management lies with BHIS.

1.3.2. BHIS provides technical user account management under direction of the BHIS Manager or designee.

1.3.3. BHIS personnel establish standard user accounts as defined by BHS Administration for each specific application.

1.3.3.1. Special access to applications (permissions greater than those required by routine users for data viewing or data entry) requires administrative review and approval by the department most responsible for the information contained or processed by the application.

1.3.4. BHIS maintains a file of appropriately signed user account forms with description of the permissions and accesses granted to each user.

1.3.5. BHIS personnel receive training on establishment and maintenance of accounts and appropriate assignment of user permissions.

1.3.6. User passwords may be reset by Community Based Programs End User Support or designated IS liaisons, only upon direct request of the user.

1.3.6.1. Supervisory personnel may request password resets for staff working 24/7 and may be provided emergency access to the information in an employee's computer files, required due to a disaster, extended leave, termination, or transfer of the employee, only upon direct request to the BHIS Manager or designee.

1.3.7. Vendor, consultant and other business associate access to systems is provided for specific time and work plans.

1.3.7.1. Vendor, consultant and other business associate access requires approval of the BHIS Manager or designee and is based on pre-defined business associate agreements and contracts.

1.3.7.2. Vendor, consultant and other business associate accesses are disabled or terminated at the end of the specified time or work plan.

1.3.7.3. Vendor, consultant and other business associate access is subject to tracking, auditing and reporting by BHIS system administrators.

1.4. Compliance and Enforcement

1.4.1. Evidence of appropriate training, supervisor authorization, and signed compliance agreement are required prior to initiation of access.

1.4.2. Where available, user access is tracked through use of audit logs reviewed by BHIS system administrators on a random, periodic basis. User audit logs are specifically reviewed for inappropriate accesses in the following circumstances:

1.4.2.1. Celebrity or notorious clients

1.4.2.2. Employees who may be clients

1.4.2.3. Client or other complaints

1.4.2.4. Reports of inappropriate access

1.4.3. Failure to comply with any part of this policy may result in termination of access to Behavioral Health Information Systems.

1.4.4. Termination of user access

1.4.4.1. User access to a specific BHIS system will be terminated after 180 days of inactivity on the account.

1.4.4.2. User access to BHIS may be terminated for cause for any of the following:

- Sharing of log-in or password,
- Providing unauthorized person or persons access to systems or data through one's log-in,
- Unauthorized disclosure of BHS data or information,
- Unauthorized use of, or access to, DPH equipment or networks,
- Accessing information for which the user is not the intended recipient,
- Failure to comply with related sections of the DPH Code of Conduct,
- Failure to comply with related DPH or BHS policies,
- Other infractions that may lead to disciplinary action,

1.4.4.3. Requirements for reinstatement of user access terminated for cause:

- Signed request or authorization from a DPH executive at the Director, Deputy Director, or Department Director level, AND
- Proof of attendance at a security training session.
- Receipt, by the employee, of more than one access termination for cause is grounds for denial of reinstatement.

2. Review Schedule

2.1. This policy is reviewed and updated according to CBHS policy procedures.

Contact Person: BHIS Manager, 415-255-3600

Distribution:
CBHS Policies and Procedures are distributed by the Office of Quality Management for Community Programs
Administrative Manual Holders
CBHS Programs
SOC Managers
BOCC Program Managers
CDTA Program Managers
SFMHP Health Information Services
ISC Directors