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: **CBHS Electronic Record Keeping**

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

Date: December 2, 2010

Manual Number: 6.00-03
References: California Health and Safety Code Sect.123149, Title 22 Sect. 70751(g)(1)(2), and Code of Federal Regulation-482.24(c) (1)(I)(ii), 42 CFR Part2

New Policy
(This policy is not intended to replace or override any Community Behavioral Health Services policies related to requirements for, or maintenance of, client medical records.)

Applicability

This policy applies to all San Francisco Community Behavioral Health Services programs that utilize electronic client record systems.

Preface:

The San Francisco Department of Public Health, Community Behavioral Health Services (CBHS) maintains electronic client records that support registration, clinical referrals, authorizations for care, provider payment activities and billing. Client specific and clinical information contained in CBHS electronic records is protected under the same regulations and guidelines that apply to other healthcare records and specifically to records of mental health and substances abuse treatment program enrollment, assessment, diagnosis, and treatment.

In health care, accurate and complete information about individuals is critical to providing high quality, coordinated care.

The… "principles established here are expected to guide the actions of all health care-related persons and entities that participate in the *[San Francisco CBHS network of care]* for the purpose of electronic exchange of individually identifiable health information. These principles are not intended to apply to individuals with respect to their own individually identifiable health information." (Excerpt from "The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information, Dec 2008.)

A. Security

1. This policy applies to all electronically processed, transferred, or stored information utilized by Community Behavioral Health Services in conduction of day to day business, including but not limited to:
   1.1. Client health information
   1.2. Client demographic information
   1.3. Client financial information
   1.4. Healthcare Provider and personnel information
   1.5. Quality Management and Utilization Review information
   1.6. Business records including strategic planning, statistical, and financial information

2. Access to electronic records is limited to authorized personnel. Authorized personnel are identified by a unique login name and verified by entry of an associated password for each information system to which they are authorized.
   2.1. Import and export of data is limited to functions implemented by authorized personnel and import from or export to data sources specifically approved by CBHS.

3. All personnel, including permanent, temporary, intern, volunteer, and contract employees are authorized through submission of a written request that:

   3.1. Is signed by the immediate supervisor.
   3.2. Provides required personal identification information.
   3.3. Identifies the specific systems and functions required for performance of duties.
   3.4. Identifies levels of training and access required by the employee and provides for tracking of training and permissions assigned.
   3.5. Requires employee signature on the forms contained here in appendix A.
   3.6. Signed access requests are maintained in a secure file for the life of the data system.

4. Authorizations

   4.1. A unique login name and password are required to access SFMHP computer systems.
   4.2. The system forces revision of the employee password every __ months.
   4.3. Passwords are encrypted and not available for look-up at any level.
   4.4. An employee may have a password reset by direct request to the System Manager.
   4.5. Passwords of employees who leave or are fired are disabled to prevent unauthorized use.

B. Confidentiality

1. Unauthorized access to or release of electronic record information is prohibited.
   1.1. Confidentiality, protection of sensitive health information, and release of client information is governed by the most current version of the CBHS Health Information Management policy and procedure: Confidentiality and Release of Information of Mental Health Records and by Code of Federal Regulations 42, Part 2 that further restricts access to Substance Abuse treatment information.

1.2. In accordance with the above policy, all employees, interns, volunteers, and contract employees who may handle client records sign an oath of confidentiality that is maintained in the individual personnel file.
1.3. Personnel are restricted from any form of unauthorized accessing or sharing of electronic client information.
1.4. Client information is not to be displayed or discussed in public areas.
1.5. Permissions to access information are restricted to the access required by the expected duties of the individual.
1.6. Provision of unauthorized access to or release of information from CBHS electronic records or data systems is prohibited and may result in disciplinary action up to and including termination of employment and may further result in civil or criminal action under the Welfare and Institutions Code, Sections 5330 and 942.

2. California State law strictly prohibits the inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment, or other lawful purpose. Further, privacy breaches must be reported to the California Department of Public Health within five days after detection.
   - Wrongful accessing of medical information may trigger any or all of the following:
     - Disciplinary action, including potential termination
     - Referral by the State to the appropriate licensing board for discipline
     - Assessment by the State of an administrative penalty of up to $25,000

C. Retention and security of electronic records

1. Retention of clinical information in electronic client records is governed by the most current version of the CBHS Health Information Management policy and procedure: Security and Retention of Medical Records with the following additions:
   1.1. Electronic records security is provided by the controlled login and password protections.
      1.1.1. Personnel receive training related to security.
      1.1.2. Personnel receive additional training related to provision of privacy for computer screens and programs.
   1.2. Electronic records are not routinely purged or destroyed.
   1.3. Substance abuse or psychiatric treatment records that require expunging are handled in accordance with Departments of Mental Health and Substance Abuse policy.
   1.4. Electronic records are stored in centrally maintained databases in a controlled environment.
   1.5. Audit logs of user access are maintained by BHIS system administrators and reviewed by CBHS QM on a random, periodic basis. User audit logs are specifically reviewed for inappropriate accesses in the following circumstances:
      1.5.1. Celebrity or notorious clients
      1.5.2. Employees who may be clients
      1.5.3. Client or other complaints
      1.5.4. Reports of inappropriate access

2. Electronic records backup occurs on a regularly scheduled basis.
   2.1. Data backup to disk is provided locally to protect against loss in the event of systems or application failure.

2.2. Database backup is stored off-site at a secure, remote location to protect records from loss or damage in the event of a disaster.

3. Downtime procedures are defined that address the anticipated impact of various levels of system failure, procedures for continuity of business, and procedures for system recovery.
   3.1. Downtime procedures are defined and implemented at the program level.
   3.2. Personnel receive training in downtime and recovery procedures.

4. Community Behavioral Health Services Information Systems is part of DPH Community Programs. DPH IS has developed and maintains a comprehensive IS Disaster plan that addresses protection and recovery of systems and data in the event of a major disaster.

D. Data integrity

1. Client information is authenticated through a search mechanism prior to entry of any data in the electronic record
   1.1. Client identification is authenticated through cross-reference with the State MediCal system, the DHS or GA system, or submission of other approved identification.
      1.1.1. The Master Patient Index resides in the primary CBHS Information System (CBHSIS).
      1.1.2. CBHSIS maintains the most accurate registration and client demographic information available and cross references known client aliases.
   1.2. Provider identification is authenticated through reference to employment information, the Provider Systems database of credentialing and through direct primary source verification of credentials.

E. Clinical information

1. The electronic record may contain clinical information that documents a client interaction with Community Behavioral Health Services.
   1.1. Records contain clinical information needed to:
      1.1.1. Document a client encounter.
      1.1.2. Document assessments, treatment plans and progress notes.
      1.1.3. Justify an authorization or denial of care.
      1.1.4. Assure continuity of care.

   1.2. Authorized personnel enter clinical information into the electronic client record.
   1.3. A clinical record may require editing to add a note after it has been saved to the record.
   1.4. Finalized clinical notes may be edited by addenda and according to medial record maintenance regulation.
   1.5. CBHSIS maintains a log of all clinical information edits that is
      1.5.1. Retrievable by the system administrator.
      1.5.2. Backed up in the full database backup system.
      1.5.3. Routinely reviewed.

1.6. Persons needing to edit clinical notes enter an addendum note with date and name indicating what was changed and the reason for the change.
1.7. In keeping with legal guidelines and CBHS policy governing medical records, clinical record notes are not completely erased. These guidelines call for corrections that permit review of the original entry with the correction.

F. Duplicate Electronic Client Records Management

1. Each client of San Francisco Behavioral Health Services and the San Francisco Mental Health Plan (SFMHP) will have one electronic record in each information system that contains correct, synchronized identifying information and the most comprehensive services information available.

2. The primary CBHS IS will be used as the Master Client Index (MPI). MPI records are updated on a regular basis and are compared to the State MEDS files for accuracy of demographic and eligibility information.

3. When duplicate records are identified
3.1. Information from both records is forwarded to CBHS Health Information Management Services (HIMS) for review and correction.
3.2. Prior to any merge activity, diagnosis and treatment information is reviewed by an authorized clinician to determine that this information is consistent with a single client's record.
3.2.1. The primary record (record to be maintained) is that record containing the most correct or complete data.
3.2.2. Registration records may be merged ad lib when last name, first name, middle name or initial, DOB and/or SSN match and when no episodes, diagnosis, services, or treatment information exists in one or both records.
3.2.3. When episodes, diagnosis, services, or treatment information is present the record with the most correct and complete information is maintained as the primary record.

Contact Person: IS Manager, CBHS. Phone: 415 255-3545

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