SAN MATEO COUNTY
MENTAL HEALTH SERVICES DIVISION

DATE: February 18, 2003; effective April 14, 2003

MENTAL HEALTH POLICY NO.: MH 03-05

SUBJECT: Disclosures of Protected Health Information (PHI), Incidental

AUTHORITY: 45 CFR 164.502(a) – Federal HIPAA Regulations; MH Policy 03-01, Confidentiality/Privacy of Protected Health Information; MH Policy 03-04, Disclosure of Protected Health Information, Minimum Necessary; County Sanctions Policy

SUPERSEDES: New Policy

ATTACHMENT: Index of HIPAA Related Policies

BACKGROUND

Federal Law permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as the covered entity has applied *reasonable safeguards* and implemented the *minimum necessary standard* where applicable, with respect to the primary use or disclosure. Examples of incidental disclosures include, but are not limited to situations where: a client in a waiting room overhears the names of other clients, clients are transported in a group for laboratory blood draws, a client observes another client leaving a medication room after receiving an injection, or a staff member sees the names of other clients while searching on the computer for a specific client's information.

PURPOSE

To define incidental disclosures and other breaches of confidentiality; to mandate *reasonable safeguards* in order to protect health information; and to provide procedural guidance concerning implementation of such safeguards.

DEFINITIONS

Incidental Disclosure – a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by HIPAA. (Note: an incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure that violated HIPAA.)

Minimum Necessary Standard The HIPAA Privacy Rule states that a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. It further requires providers to identify those in the workforce who need access to client information, to determine how much access is necessary to perform the work function, and to limit access accordingly. In general, the minimum necessary rule does not apply to the disclosure of health information between treating providers.

POLICY

Mental Health Services shall have in place, in every clinical and administrative site, appropriate administrative, technical and physical safeguards to protect against uses and disclosures not permitted by HIPAA, and to limit incidental uses and disclosures. The Index of HIPAA Related Policies (Attached) is included as a general reference to policies concerning confidentiality of protected health information.

Mental Health Services shall provide training for all staff in basic principles of confidentiality concerning protected health information, and in the specific policies and procedures developed to protect client confidentiality. As necessary, Mental Health Services shall also provide training on policies originating at the County or Departmental level concerning data security, confidentiality, staff responsibility and sanctions, and other related topics.

It is the responsibility of all staff to understand these policies and procedures and follow their mandates with scrupulous attention. It is further the responsibility of all staff to make a good faith effort to reduce or eliminate incidental disclosures as these are identified.

PROCEDURES

Protocols concerning medical record management, authorization of disclosures, etc., are covered in the policies referenced in the attached Index and in other policies already in practice. HIPAA requires that we follow these good practice policies.

Security of Protected Health Information – While HIPAA Security Regulations are not yet in place, any aspect of security that impacts Confidentiality/Privacy of PHI must be reviewed and reasonable safeguards taken to minimize incidental disclosures. The following procedural list includes but does not limit common areas with high risk for disclosure of PHI.

A. All protocols for safety of electronic information (password protection, shutting down PC's when not in use, security of hand-held devices, etc.) shall be followed.

B. All protocols for securing the medical record (in file rooms and/or locked files, working-chart file containers that do not disclose client names, no clients' charts left on clinician desks such that they can be seen by other clients, chart locked away when not in use, no charts taken to a staff member's home, etc.) shall be followed

C. Lead administrative and clinical staff at each site shall survey that site and shall take steps to assure that:

1. Computer screens displaying PHI are not readily visible to visitors, clients, family members and others.
2. Fax machines and printers are located in such a manner that PHI is not readily visible to visitors, clients, family members and others.

D. Each site shall analyze the traffic flow at the front (registration) desk and consider establishing a "wait here" policy or other system to allow an amount of privacy for the person registering for an appointment.

E. Methods of calling clients from group waiting rooms shall be evaluated to minimize the disclosing of complete names (such as, therapist walking up to waiting client, using first names with permission of the client, etc.)

F. All conversations with clients concerning PHI, in common areas such as hallways, shall be conducted quietly.

G. Administrative and clinical staff shall be trained to protect the identity of the client being spoken to by telephone to the greatest possible extent.

H. Financial interviews with clients shall take place with the maximum privacy the site allows.

I. Telephone messages may be left for clients but care shall be taken to minimize the information left on an answering machine or given to someone else in the household.

Approved: _____

Gale Bataille, Director
Mental Health Services Division