POLICY TITLE: Clinical Data Security

Effective January 1, 1996

INTRODUCTION

In addition to the confidentiality safeguards used for recording, storage, communication, and retrieval of recorded service delivery data on hard copy (paper), the following additional steps and clarifications are in effect to assure confidentiality of both hard copy and electronically processed information. This policy applies to all staff and program sites within the Alameda County Behavioral Health Care Services System, both County-operated and contracted sites.

RESPONSIBILITIES AND AUTHORIZATIONS

1) It is the Center Director's / Executive Director's responsibility to assure that all access to information is in compliance with Section 5328 of the Welfare and Institutions Code (programs funded through the Mental Health Services Division) and/or the Code of Federal Regulations (42 CFR) Part 2 (programs funded through the Alcohol and Drug Services Division).

2) Staff may only use the lookup/inquiry feature of the PSP system to access information about clients for whom they have some degree of service delivery responsibility. (As with hard copy records, access is also authorized for clerical staff acting on behalf of those with service delivery responsibility.) Attempts to access client information beyond the scope of this service delivery need to know is against ACBHCS policy and outside the scope of a staff member's job duties. Such attempts will be subject to disciplinary action. Legal actions arising out of such breeches of confidentiality will not be protected by the County's liability or malpractice insurance coverage.

3) Any staff violation of Section 5328 of the W and I Code and/or 42CFR, Part 2 in the misuse of electronically based information is subject to the same penalties and disciplinary actions as applies to hard copy clinical data. Violations shall be noted in the respective personnel record and will be subject to appropriate corrective action.

4) A staff member's authorization level will determine the kinds of information they may access from the computer. The assignment of authorization levels will be recommended by supervisory staff on the basis of each staff members need to know, and it is subject to the Center Director /Executive Director's approval.

5) It is a violation of ACBHCS policy for a staff member to make their password known to any other individual. Anyone who has made their password known to others must establish a new confidential password immediately.

DATA PROCESSING SECURITY

1) No service delivery files may be downloaded onto PC's or floppy disks except by approval of the Quality Assurance Administrator, ACBHCS Office of Management Services.

2) Video monitors in public places (for example, clerical areas through which clients and visitors might pass on their way to offices) shall be positioned so that they are not viewable to passersby. (The same policy applies to hard copy left open on desks in public places.)

3) If a terminal must be left unattended, the user must either use the "terminal lock" security feature or log off in order to prevent unauthorized access.

CLIENT ISSUES

1) If any client achieves exceptional notoriety or celebrity so as to create an exceptional risk of confidentiality breach, their files shall be blocked from general lookup (inquiry) access. The Center Director/Executive Director shall notify the ACBHCS Data Processing Unit which will change the client's electronic file to a code name. Similarly, such a client's hard copy files will be removed from the general clinic file cabinet and kept under special security arrangements by the Center Director/Executive Director.

2) All clients shall be informed about the general nature of confidentiality under applicable State law and/or Federal regulations, both its protections and its limitations, as relevant and whenever possible.

PLEASE NOTE: THIS POLICY IS CURRENTLY UNDER REVISION- April 8, 2010