

County of San Bernardino Department of Behavioral Health

User- I.D. and Password Policy

Effective Date 01/29/2007
Revised Date 10/26/2010


 Allan Rawland, Director

Policy The Department of Behavioral Health (DBH) will use standardized User Identifications (User-I.D.)s and complex passwords to protect its systems and data from unauthorized access in accordance with Departmental, County, State, and Federal requirements to preserve the confidentiality of Protected Health Information (PHI) and/or Personally Identifiable Information (PII) electronic data.

Purpose To establish staff responsibilities and a method for tracking data access by the issuance of User-I.D.'s and complex passwords, which will protect the integrity, vulnerability, and unauthorized access of PHI and/or PII data.

General Information Staff requiring access to DBH systems will be assigned one or more unique User-I.D.'s based on daily job duties. Each User-I.D. will have a unique complex password that must not be shared between staff.

Staff Responsibilities The following are the responsibilities of the staff:

Staff	Responsibilities
Manager/Supervisor	<ul style="list-style-type: none"> • Request staff authorizations in writing on the Information Services (IT) Network User Request/Update form and provide: <ul style="list-style-type: none"> ○ Employee name ○ Employee county identification number ○ Unit or clinic to which employee is assigned ○ Application(s) to which access is required ○ Level of responsibility and need to know confidential client information • Notify IT on the IT Network User Request/Update form if there is a change to an employee's level of responsibility

Continued on next page

County of San Bernardino Department of Behavioral Health

User- I.D. and Password Policy, Continued

Staff Responsibilities (continued)

Information Technology	<ul style="list-style-type: none"> • Establish a User-I.D. and first-time temporary password for network access for new staff members only • Establish a User-I.D. and first time temporary password for each requested application based upon level of responsibility • Notify staff member of assigned User-I.D. and temporary password • Reset staff passwords which have been compromised or forgotten • Disable, reestablish, or terminate a staff member's access based upon a request from management by e-mail, telephone or the IT Network User Request/Update form • Notify the department's Compliance Officer of each access granted and removed
Staff	<ul style="list-style-type: none"> • Select a new password when prompted upon initial sign-on to the network and/or application • Create a Password with a minimum length of eight characters and which contain two of the three following characteristics: <ul style="list-style-type: none"> ○ One upper and lower case alphabetic character ○ One numeric character ○ One special character such as; \$, #, @ • Keep all passwords secure • Change passwords every ninety (90) days or when prompted by the system • Notify IT when locked out of the system and a password reset is required
Management/Human Resources	<p>Notify IT in writing via the weekly HIPAA report when a staff member's access should be terminated, disabled, or reinstated.</p> <p>Note: Verbal notification is acceptable if action is to be taken immediately.</p>

Continued on next page

County of San Bernardino

Department of Behavioral Health

User- I.D. and Password Policy, Continued

Consequences of Violations Staff violating the use of DBH systems as described above or in other County policies will be subject to disciplinary action that can include termination of employment.

References Code of Federal Regulations 42, Part 431.300, Section 2.1 et seq.
Code of Federal Regulations 45, Parts 160 and 164.
California Civil Code 56 et seq. (The Confidentiality of Medical Information Act)
California Health and Safety Code (Information Practices Act of 1977), Section 1798 et seq., Section 123100 et seq. (Client Access to Health Records)
California Welfare and Institutions Code, Sections 5328 et seq., 14100
Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, Privacy Rule (HIPAA)
Department of Behavioral Health Medi-Cal Privacy and Security Agreement

Related Policy or Procedure County of San Bernardino Policy Manual 14-01: [Electronic Mail \(E-mail\) Policy](#)
County of San Bernardino Policy Manual 14-04: [Internet/Intranet Use Policy](#)
County of San Bernardino Policy Manual 16-02: [Protection of Individually Identifiable Health Information](#)
County of San Bernardino Policy Manual 16-02SP1: [Protections of Individually Identifiable Health Information](#)
DBH Standard Practice Manual IT5003: [Internet Account Policy](#)
DBH Standard Practice Manual IT5004: [Computer and Network Appropriate Use Policy](#)
DBH Standard Practice Manual IT5005: [Electronic Mail Policy](#)
DBH Standard Practice Manual IT5006: [Remote Access Policy](#)
DBH Standard Practice Manual IT5008: [Device and Media Controls Policy](#)
