

**County of San Bernardino
Department of Behavioral Health**

Privacy or Security Breach Policy

Effective Date 07/01/2010
Approval Date 10/26/2010



Allan Rawland, Director

Policy The Department of Behavioral Health (DBH) shall adhere to state and federal regulations pertaining to the reporting of privacy and/or security breaches.

Purpose Provide the DBH workforce with guidance on the requirements for identifying a breach, individual responsibility for reporting a breach, and how to report a breach to the DBH Office of Compliance immediately upon discovery.

Definitions

Assist in the Administration of the Medi-Cal Program: Performing an administrative function on behalf of Medi-Cal, such as verifying Medi-Cal eligibility of a client.

Breach: Unauthorized access, use or disclosure of personally identifiable information or protected health information that violates state or federal privacy or security laws.

Medi-Cal PII: Information directly obtained from MEDS in the course of performing an administrative function on behalf of Medi-Cal that can be used alone, or in conjunction with other information to identify a specific individual.

Personally Identifiable Information (PII): Any piece of information maintained by DBH electronically or in paper format which can potentially be used to uniquely identify, contact or locate County employees or members of the public.

Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained in any form or medium (electronic, paper, microfiche or verbal)

Unauthorized Access: Inappropriate/impermissible entry, contact, review, opening or viewing of employee, public or client information without direct need for medical diagnosis, treatment, business purpose or other lawful use and any other unlawful use not permitted by state or federal laws governing the use or disclosure of confidential information, medical or otherwise personal.

Unauthorized Disclosure: Inappropriate/impermissible release, announcement, publication or statement of employee, public or client information without direct need for medical diagnosis, treatment, business purpose or other lawful use and any other unlawful release not permitted by state or federal laws governing the use or disclosure of confidential information, medical or otherwise personal.

Continued on next page

County of San Bernardino

Department of Behavioral Health

Privacy or Security Breach Policy, Continued

Definitions (continued)

Unauthorized Use: Inappropriate/impermissible handling, application, operation or management of employee, public or client information without direct need for medical diagnosis, treatment, business purpose or other lawful use and any other unlawful application not permitted by state or federal laws governing the use or disclosure of confidential information, medical or otherwise personal.

DBH Workforce: County employees, paid and unpaid interns, contractors and contract agencies that provide clinical or administrative services for the Department of Behavioral Health.

Identification of a Breach

The following are examples of actions that may be privacy or security breaches. Staff is required to report to the DBH Office of Compliance immediately upon discovery. Examples include, but are not limited to the following:

- Faxing or emailing PHI/PII to the wrong recipient
- Emailing PHI/PII to anyone outside the County network, including yourself
- Sending correspondence to the incorrect client
- Releasing PHI/PII to a person or entity with an expired [Authorization for Release of Protected Health Information](#)
- Misplacing/losing a medical record after a thorough search
- Accessing/using DBH and/or County resources to verify if family, friends or acquaintances are DBH clients
- Accessing, using or disclosing information obtained from MEDS to contract providers
- Accessing, using or disclosing information obtained from MEDS other than to assist in the administration of the Medi-Cal Program
- Accessing/peeking in a medical record you did not need to access for a legitimate business purpose or to perform your job
- Being the victim of theft where DBH medical records or DBH property are taken
- Leaving medical records or PHI/PII in an unattended vehicle
- "Checking in" medical records or PHI/PII on modes of public transportation; not keeping it/them in personal custody as carry on
- Giving yours or using others' password/log in
- Leaving medical records or PHI/PII unsecured, i.e.; open and unattended on the desk, unlocked medical charts, unlocked PII, etc.
- Allowing unauthorized persons in the work area without a legitimate business purpose
- Discussing with or disclosing to others PHI/PII without a legitimate business purpose and/or without authorization from the client
- Discarding PHI/PII or medical records improperly and/or not in accordance with retention timeframes

Continued on next page

County of San Bernardino Department of Behavioral Health

Privacy or Security Breach Policy, Continued

Identification of a Breach (continued)

Important Note: The above examples may include inadvertent errors, negligence or even malicious intent. However, no matter the degree of access, use or disclosure, the DBH Office of Compliance must investigate the breach.

Responsibilities and Reporting a Breach

There are various state agreements and state/federal regulations guiding the DBH Office of Compliance as to breach reporting requirements, including time frames. Due to the varied requirements, the following table illustrates the responsibility of the applicable DBH Workforce:

Responsible Party	Responsibility
DBH Workforce	<ul style="list-style-type: none"> • Report any act that appears to be a breach immediately when discovered to: DBH Office of Compliance Office (909) 382-3083 Hotline (800) 398-9736 • Email Compliance_Questions@dbh.sbcounty.gov
DBH Contract Agencies	<ul style="list-style-type: none"> • Adhere to the Business Associate Agreement regarding reported breaches within its agency: <ul style="list-style-type: none"> – Reporting to DBH within the required timeframe – Investigating the reported breach – Reporting the findings to DBH
DBH Office of Compliance	<ul style="list-style-type: none"> • Notify applicable state agency(ies), as required • Investigate facts of the breach, which may include but are not limited to the following: <ul style="list-style-type: none"> – Conducting interviews with employee(s) and/or individuals involved, as necessary – Gathering documentation, data, etc. – Verifying what data was breached • Determine if a breach has or has not occurred • Notify the client(s) affected by the breach, as required • Prepare formal breach report for applicable agency(ies) • Issue memo to applicable deputy director and program manager including recommended corrective action, if applicable • Provide guidance to applicable program, as needed • Follow-up with program to ensure corrective actions are completed and/or addressed
DBH Program	Complete corrective action, if applicable

Continued on next page

County of San Bernardino

Department of Behavioral Health

Privacy or Security Breach Policy, Continued

Violations	<p>Members of the DBH Workforce may be subject to the following actions due to a breach:</p> <ul style="list-style-type: none">• Corrective action including but not limited to receiving re-training on privacy and security measures, reviewing existing policy and signing policy acknowledgement forms• Loss of MEDS access• Disciplinary action, up to and including termination of employment• Civil or criminal liability
-------------------	---

Note: The action taken in response to a breach will be based on the violation levels as indicated in the [HIPAA Violation Sanctions Policy](#).

Failure to Report	<p>The omission or failure to report a breach may subject members of the DBH Workforce to disciplinary action, up to and including termination.</p>
--------------------------	---

References	<p>California Civil Code, Section 56 et al., California Confidentiality of Medical Information Act Medi-Cal Privacy and Security Agreement Social Security Act, Sections 1137 and 453 Title 45 of the Code of Federal Regulations, Section 164 et al., Health Insurance Accountability and Portability Act of 1996 Welfare and Institutions Code, Section 14100.2</p>
-------------------	---

Related Policies and Procedures	<p>County of San Bernardino Policy Manual, 16-01, Non-Public Personally Identifiable Information County of San Bernardino Policy Manual, 16-02, Protection of Individually Identifiable Health Information County of San Bernardino Standard Practice, 16-02SP1, Protection of Individually Identifiable Health Information DBH Standard Practice Manual, COM0943-1, MEDS Access and Contacts Procedure DBH Standard Practice Manual, IT5009, User I.D. and Password Policy DBH Standard Practice Manual, COM0901, Sending Confidential Information by Facsimile Policy DBH Standard Practice Manual, IT0909, Electronic Transfer of Client Protected Health Information – Internet and Intranet Policy DBH Standard Practice Manual, IT5008, Device and Media Controls Policy DBH Standard Practice Manual, COM0907, Unauthorized Access of Confidential Medical Records Policy DBH Standard Practice Manual, COM0924, Workstation and System Security Policy DBH Standard Practice Manual, COM0925, Data Integrity Policy</p>
--	---

Continued on next page

**County of San Bernardino
Department of Behavioral Health**

Privacy or Security Breach Policy, Continued

**Related
Policies and
Procedures**
(continued)

DBH Standard Practice Manual, COM0926, [HIPAA Violation Sanctions 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, COM0905, [Client Privacy and Confidentiality](#)
