SAN BERNARDINO COUNTY
Behavioral Health
303 E. Vanderbilt Way San Bernardino | (909) 388-0900
www.SBCounty.gov

Privacy Incident Policy

Effective Date	07/01/2014
Revised Date	10/14/2025

Signed by: Dr. Gayani DeSilva 4F7918C8B04426 — Dr. Gayani DeSilva
On behalf of Georgina Yoshioka, DSW, MBA, LCSW, Director

Policy

It is the policy of the Department of Behavioral Health (DBH) to ensure DBH staff and contract providers adhere to state and federal regulations pertaining to the reporting of privacy and/or security incidents, including breaches. DBH requires workforce members to immediately report privacy incidents or potential breaches of PHI to the DBH Office of Compliance (Compliance) and their supervisor upon discovery.

Purpose

To communicate individual responsibility for reporting an incident involving DBH client protected health information (PHI) to the DBH workforce and to provide information and instruction on the requirements for identifying and reporting a privacy or security incident to DBH Compliance promptly upon discovery, as well as direction for taking necessary mitigative action(s).

Definitions

Breach: Acquisition, access, use or unauthorized disclosure of protected health information in a manner not permitted under the Health Insurance Portability and Accountability Act, which compromises the security or privacy of the information. An impermissible use or disclosure is presumed to be a breach unless the covered entity demonstrates a low probability that the information has been compromised or falls under one of three exceptions as specified in 45 CFR §164.400-414.

Electronic Health Record (EHR): A digital repository of a client's medical information that documents all healthcare information in real time (DBH uses myAvatar).

Personally, Identifiable Information (PII): Information that can be used alone or in conjunction with other personal or identifying information, which is linked or linkable to a specific individual. This includes: name, social security number, date of birth, address, driver's license, photo identification, other identifying number (case number, client index number, medical record number, etc.).

Privacy Incident: An event involving the impermissible use or disclosure of PHI (this may include a security incident involving ePHI). May also involve a violation of a DBH or County protocol or policy/procedure relating to confidentiality, privacy and/or security of PHI.

Continued on next page

Definitions, continued

Protected Health Information (PHI): PHI is *individually identifiable health information* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral. Individually identifiable information is information, including demographic data, that relates to the individual's past, present or future physical or mental health or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual, and identifies the individual or for which there is reasonable basis to believe it can be used to identify the individual. PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; in records described at 20 U.S.C. 1232g(a)(4)(B)(iv); in employment records held by a covered entity in its role as employer; and regarding a person who has been deceased for more than fifty (50) years.

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of ePHI or interference with information system operations.

Snooping: Unauthorized viewing of PHI or ePHI for non-business reasons (i.e., unrelated to treatment, payment or operations).

Unauthorized Access: Inappropriate/impermissible entry, contact, review, opening or viewing of client PHI without business need.

Unauthorized Disclosure: Revealing or sharing client PHI without proper authorization or legal exception to the authorization requirement.

Unauthorized Use: Acquisition, access, use or disclosure of client PHI without business need or proper authorization.

Workforce Member(s): Employees, volunteers, trainees, students, interns, contracted providers and their staff, and other persons, paid or unpaid, whose conduct, in the performance of work for DBH, is under the direct oversight and requirements of the DBH Code of Conduct.

Continued on next page

Identification of a Privacy or Security Incident

The following are examples of actions that may be privacy and/or security incidents. Workforce members are required to report any of these to 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 DBH or contract provider network, without encryption (password protection is not encryption);
- Using personal devices to transmit or store client PHI;
- Sending a correspondence to the incorrect client;
- Releasing PHI/PII to a person or entity with an invalid or incomplete 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, or snooping into, a medical record without a legitimate business purpose or need to perform your job;
- Being the victim of theft where DBH medical records or DBH technology are taken;
- Leaving medical records or PHI/PII unattended (e.g. vehicle, printer or fax machine, conference room);
- Leaving medical records or PHI/PII unsecured, i.e.; open and unattended on the desk, unlocked medical charts, unlocked vehicle etc.
- "Checking in" baggage containing medical records or PHI/PII on modes of public transportation;
- Using another's credentials to access the DBH network/myAvatar or letting someone else use yours;
- 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.

Guidance on reporting incidents involving a client's Electronic Health Record (EHR):

- A privacy incident is considered to have occurred when a DBH client's PHI is disclosed or put at risk of being accessed without authorization and does not meet the requirements of an exception under the law. The most common ways this occurs in the EHR are:
  (1) Errors made during process of scanning documents into charts,
  (2) Misfiling documents under the wrong client or program assignment (e.g. filing a substance abuse record in a mental health category), and,
  (3) Mixing different client's data within the same document.

Continued on next page

Identification of a Privacy or Security Incident, continued

Addressing corrections in the EHR:

- All errors caught by a workforce member in real-time or during self-check stage may be corrected immediately (with assistance as needed) and **do not** need to be reported to Compliance.
- All errors discovered later than the time of document completion/scanning, or by other persons after the time of completion, **shall be reported** to Compliance **immediately upon discovery.**
- Mediation to remove/prevent further inappropriate disclosure of the PHI must be initiated immediately upon identification of the error and included in the report to Compliance.

Important Note: The above examples may include inadvertent errors, negligence or even malicious intent, no matter the degree of access, use or disclosure, Compliance must investigate the incident to determine if the incident is a privacy policy violation or a breach reportable to the state and federal government.

Breach Reporting Requirements

The HIPAA Breach Notification Rule

- The HIPAA Breach Notification Rule requires covered entities and business associates to notify affected individuals, the Secretary of Human Services, and, in certain cases, the media, following a breach of unsecured protected health information (PHI).
- Client notifications must be provided without delay and no later than 60 days after discovering the breach. Business associates must also notify covered entities if a breach occurs at or by the business associate.
- Substance Use Disorder (SUD) PHI covered under 42 CFR Part 2 must adhere to the same HIPAA breach reporting requirements as Mental Health PHI.

Continued on next page

Role and Responsibilities for Reporting an Incident or Breach

The following table illustrates the responsibility of Workforce Members for reporting suspected/actual breaches:

Role	Responsibility
Workforce Member(s)	• Report any privacy/security incident immediately, but not later than the date discovered; • Submit the **Privacy and Security Incident Reporting Form** (COM042) at the time of reporting to DBH-PrivacyIncidents@dbh.sbcounty.gov; • Attempts to mitigate the potential for unauthorized access must be implemented immediately; • For guidance, call: DBH Office of Compliance (909) 383-3991.
DBH Contract Agency Workforce Member(s)	• Adhere to the DBH contract requirements regarding reporting possible breaches to DBH Compliance • Complete and submit the **Privacy and Security Incident Reporting Form** and submit to DBH-PrivacyIncidents@dbh.sbcounty.gov; • Investigate the possible breach internally: ○ Coordinate with DBH Compliance to notify applicable state agency(ies), as required. ○ Promptly communicate and coordinate with any agency subcontractors involved directly or indirectly with unauthorized access to PHI;
DBH Contract Agency Workforce Member(s). continued	• Investigate facts of the privacy/security incident, which may include but are not limited to the following: ○ Conducting interviews with employee(s) and/or individuals involved, as necessary; ○ Gather documentation, data, etc; ○ Verifying what information was at risk of compromise; ○ Provide DBH Compliance timely and necessary information to determine if a reportable breach has occurred; ○ Notify the client(s) affected by the breach as required by regulation and upon guidance by DBH Compliance, and • Report the findings to DBH Compliance.

Continued on next page

Role and Responsibilities for Reporting an Incident or Breach, continued

Role	Responsibility
DBH Compliance	• Monitor reporting of privacy incidents and/or potential privacy breaches; • Promptly respond to staff whom provided reporting and assign internally for investigation/assessment; • Ensure a risk assessment is performed on appropriate incidents; • Ensure HIPAA Security Officer and appropriate Information Technology staff are apprised of all security incidents and address, evaluate and assess mitigation efforts; • Make all reasonable efforts to recover or destroy any hardcopy or electronic PHI disclosed to an unauthorized user to minimize the risk of harm to the individual(s) subject to the incident; • Oversee contract provider response measures to ensure all contractual obligations are completed and timely; • Facilitate the acquisition of mitigating attestations of deletions and non-disclosure(s); • Prepare formal incident report for applicable agency(ies); • Issue memo to applicable supervisor, manager and/or deputy director or designee including corrective action plan (CAP), if applicable (include DBH HR for advisement purposes); • Provide guidance to applicable program, as needed, and • Follow-up with program to ensure corrective actions are completed and/or addressed.
DBH Program	• Complete corrective action(s), as/if applicable or instructed per Compliance Memo.

Violations

Workforce Member(s) may be subject to the following actions due to a privacy violation:

- Corrective action, including but not limited to receiving re-training on standards, privacy and security measures; reviewing existing policies and procedures and signing acknowledgement forms;
- Loss of MEDS access;
- Disciplinary action, up to and including termination of employment, and
- Civil and/or criminal liability.

Note: The action(s) taken in response to a privacy incident or breach will be based on the violation levels, as well as recurrence of violation(s), as indicated in the Privacy and Security Violation Sanctions Policy.

Continued on next page

Failure to Report

The omission or failure to report a privacy or security incident may subject workforce members to disciplinary action, up to and including termination.

Related Policies and Procedures

County of San Bernardino Policy Manual:

- Non-Public Personally Identifiable Information (14-02)
- Protection of Individually Identifiable Health Information (14-03)
- Protection of Individually Identify able Heal the Information (14- 03SP1)

DBH Standard Practice Manual and Departmental Forms:

- Privacy and Security Incident Reporting Form (COM042)
- Sending Confidential Information by Facsimile Policy (COM0901)
- Confidentiality of Protected Health Information (PHI) (COM0905)
- Unauthorized Access of Confidential Medical Records Policy (COM0907)
- Workstation and System Security Policy (IT5022)
- Privacy and Security Incident Sanctions Policy (COM0926)
- Computer and Network Appropriate Use Policy (IT5004)
- Electronic Mail Policy (IT5005)
- Remote Access Policy (IT5006)
- Device and Media Controls Policy (IT5008)
- User I.D. and Password Policy (IT5009)
- DBH-IT Data Encryption Policy (IT5018)

References

- California Civil Code, § 56 et al., (California Confidentiality of Medical Information Act)
- Health Insurance and Portability Act (HIPAA) (Title 45 Code of Federal Regulations Part 160 and 164 Subparts A and E)
- Medi-Cal Privacy and Security Agreement
- Social Security Act, § 1137 and 453
- The Health Information Technology for Economic and Clinical Health (HITEH) Act
- Title 42 Part 2 of the Code of Federal Regulations
- Welfare and Institutions Code, § 14100.2