Privacy Incident Policy

Effective Date	07/01/2014	DocuSigned by: Dr. Georgina Yoshioka Interim Director 7DF8077EFA674B2...
Revised Date	10/25/2022	Georgina Yoshioka, DSW, MBA, LCSW, Interim Director

Policy

It is the policy of the Department of Behavioral Health (DBH) to adhere to state and federal regulations pertaining to the reporting of privacy and/or security incidents, including breaches. If a workforce member discovers a privacy incident or potential breach of PHI, they must immediately report the incident to the DBH Office of Compliance (Compliance) and their supervisor.

Purpose

To provide workforce members with guidance on the requirements for identifying a privacy or security incident; communicate individual responsibility for reporting an incident; and outline how to report an incident to DBH Compliance promptly upon discovery and take any necessary mitigative action(s).

Definition(s)

Breach: The acquisition, access, use, or disclosure of protected health information in a manner not permitted by HIPAA (45 CFR §164.402), 42 CFR Part 2 or WIC §5328, which compromises the privacy and confidentiality of protected health information. DBH Compliance is responsible for determining if a privacy incident is a breach and/or is reportable to the state and/or federal government, based on completed research, evaluation and risk assessment.

Medi-Cal Personally Identifiable Information (M-PII): Information directly obtained from Medi-Cal Eligibility Data System (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): 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 incident involving the impermissible use or disclosure of PHI (this may include a security incident in which ePHI is relevant). Within DBH, a privacy incident may also entail a protocol or County or DBH policy/procedure violation relating to confidentiality, privacy and/or security of PHI.

Continued on next page

Privacy Incident Policy, Continued

Definition(s), continued

Protected Health Information (PHI): 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; past, present or future physical or mental health or condition; the provision of health care to a client; or the past, present or future payment or the provision of health care to a client.

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

Snooping: Unauthorized viewing of PHI (particularly in the Electronic Health Record) for non-business reasons (i.e., unrelated to treatment, payment or operations).

Unauthorized Access: Inappropriate/impermissible entry, contact, review, opening or viewing of client information without direct need, such as 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 client PHI without direct need, such as 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.

Unauthorized Use: Inappropriate/impermissible handling, application, operation or management of client information without direct need, such as 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.

Workforce Member(s): Employees, volunteers, trainees, students, interns, 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

Privacy Incident Policy, Continued

Identification of a Privacy or Security Incident

The following are examples of actions that may be privacy and possibly security incidents as well. Staff 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 County network, including yourself, without encryption (password protection is not encryption);
- 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 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 technology are taken;
- Leaving medical records or PHI/PII unattended (e.g. vehicle, conference room);
- Leaving medical records or PHI/PII unsecured, i.e.; open and unattended on the desk, unlocked medical charts, unlocked PII, etc.
- "Checking in" baggage containing medical records or PHI/PII on modes of public transportation; not keeping it/them in personal custody as carry on;
- Using another's credentials 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

Privacy Incident Policy, Continued

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.

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

Role and Responsibilities for Reporting an Incident or Breach

Various state agreements and state and federal laws establish breach-reporting requirements, including reporting timeframes. DBH must adhere to these established requirements, and Compliance is responsible for ensuring DBH maintains adherence. Due to the varied requirements, the following table illustrates the responsibility of Workforce Member(s):

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 regarding reporting possible breaches within its agency: 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;

Continued on next page

Privacy Incident Policy, Continued

Role and Responsibilities for Reporting an Incident or Breach, continued

Role	Responsibility
DBH Contract Agency Workforce Member(s). continued	• Investigate facts of the privacy/security incident, which may include but are not limited to the following: o Conducting interviews with employee(s) and/or individuals involved, as necessary; o Gather documentation, data, etc; o Verifying what information was at risk of compromise; o Provide DBH Compliance **timely and necessary information** to determine if a reportable breach has occurred; o Notify the client(s) affected by the breach as required by regulation and upon guidance by DBH Compliance, and o Report the findings to DBH Compliance.
DBH Compliance	• Monitor reporting of privacy incidents and/or potential privacy breaches; • Promptly respond to staff whom provided reporting and assign 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.

Privacy Incident Policy, Continued

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.

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 al Information on by Facsimile Policy (COM0901)
- Client Privacy and Confidentiality of Protected Health (COM0905)
- Unauthorized Access of Confidential Medical Records Policy (COM0907)
- Electronic Transfer of Client Protected Health Information- Internet and Intranet Policy (COM0909)
- Workstation and System Security Policy (COM0924)
- Data Integrity Policy (COM0925)
- Privacy and Security Violation Sanctions Policy (COM0926)
- MEDS Access and Contacts Procedure (COM0943-1)
- 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)

Continued on next page

Privacy Incident Policy, Continued

References

- California Civil Code, Section 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, Sections 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, Section 14100.2