Privacy and Security Incident Sanctions Policy

Effective Date 11/17/2006
Revised Date 06/17/2025

DocuSigned by: Dr. Georgina Yoshioka 7DF807EFA674B2...
Georgina Yoshioka, DSW, MBA, LCSW, Director

Policy

It is the policy of the Department of Behavioral Health (DBH) to take appropriate actions for DBH staff and contract providers who violate federal, state, and departmental privacy or security laws/regulations, including, but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and that staff understand they have a duty to report violations without fear of reprisal per the DBH Code of Conduct.

Purpose

To provide information and instruction to ensure all members of the DBH workforce including, but not limited to DBH staff, volunteers, interns and contractor employees, are aware of sanctions that apply to those who violate privacy and security requirements, including, but not limited to, HIPAA Privacy and Security Rules, DBH privacy and security policies, and the Medi-Cal Privacy and Security Agreement.

Definition

Breach: An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of Protected Health Information (PHI).

Privacy/Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or interference with system operations in an information system that does not result in a breach.

Violations

Listed below are the types of violations that may require disciplinary action by DBH subject to the severity of the violation and level of culpability.

Level	Description of Violation
1	**Accidental or Unintentional**: This level of breach occurs when an employee unintentionally or carelessly accesses, reviews or reveals client PHI to themselves or others without a legitimate need-to-know. Individual did not know they violated a privacy or security requirement or policy, such as but not limited to the following: • Accessing information not needed to do job. • Failure to safeguard passwords or login information. • Leaving computer unlocked and unattended while logged into a program containing PHI. • Leaving PHI unlocked and unattended while away from desk.

Continued on next page

Violations (continued)

Level	Description of Violation
1 (Cont'd)	• Discussing and/or disclosing confidential or client information with unauthorized persons. • Copying or altering PHI without written authorization or direct business need. • Misdirecting faxes or emails that contain PHI. • Discussing confidential client information in a public area or in an area where the public could overhear the conversation. • Failure or refusal to cooperate with the DBH Chief Compliance Officer, Privacy or Security Officer, or authorized designee regarding a privacy or security investigation.
2	**Deliberate violation**: This level of breach occurs when an employee intentionally accesses or discloses PHI in a manner inconsistent with DBH policies and procedures, but for reasons unrelated to personal gain. Individual did know they violated a privacy or security requirement or policy. The privacy or security violation was due to reasonable cause and not wilful neglect, such as but not limited to the following: • Second occurrence of any Level 1 offense (does not have to be the same offense). • Unauthorized use or disclosure of PHI. • Using another person's computer access code (username and password, authorized or not by the user). • Sharing computer access codes (username and/or password). • Failure or refusal to comply with a remediation resolution or recommendation.
3	**Wilful neglect and malicious violation:** This tier of breach occurs when an employee accesses, reviews or discloses PHI for personal gain or with malicious intent. A conscious, intentional failure or reckless indifference to the obligation to comply with privacy or security policies or violation with intent to harm. • Third occurrence of any level 1 offense (does not have to be the same offense). • Second offense of any level 2 offense (does not have to be the same offense). • Leaving PHI in a public area. • Obtaining confidential information under false pretences. • Using and/or disclosing confidential information for commercial advantage, personal gain or malicious harm.

Possible Disciplinary Actions

Any violation of DBH privacy and security policies, and/or related state or federal laws governing the protection of confidential and client protected health information (PHI) may result in disciplinary action as indicated in the table below.

Continued on next page

Possible Disciplinary Actions (continued)

Violation Level	Recommended DBH Disciplinary Action
1	• Verbal or written reprimand depending on severity of the violation. • Retraining on privacy/security awareness. • Retraining on DBH privacy and security policies. • Retraining on the proper use of internal controls and required forms.
2	• Consider Disciplinary Actions taken for Level 1 violations, which may be combined with additional actions below if appropriate. • Letter of Reprimand, or suspension depending on severity of the violation. • Retraining on potential civil and criminal prosecution associated with privacy and security violations.
3	• Consider Disciplinary Actions taken for Level 1 and/or Level 2 violations, which may be combined with additional actions below if appropriate. • Disciplinary action, up to and including termination of employment or contract. • Retraining on potential civil and criminal prosecution associated with privacy and security violations.

Important Note: The potential disciplinary actions are intended to provide guidance in policy enforcement and are not meant to be all-inclusive. If a Letter of Reprimand or formal discipline is deemed necessary, the DBH manager/supervisor shall consult with the Human Resources Business Partner (HRBP) prior to taking action. When appropriate, progressive disciplinary action steps shall be followed allowing the employee an opportunity to correct the behavior which caused the disciplinary action.

Exceptions

Depending on the severity of the violation, the department may take more severe disciplinary action against an employee who has committed any single act or omission resulting in disciplinary action up to and including termination of employment or contract with DBH.

Continued on next page

Penalties and Sanctions

Civil or criminal prosecution penalties up to $1.8 million may apply as provided under HIPAA, 42 CFR Part 2, or other applicable Federal, State, or local laws. DBH may be required to report employee privacy/security violations to applicable licensing boards via a health facility/peer review report. Licensing Boards may also impose disciplinary actions such as cost recovery, suspension, or revocation/denial of license or registration (see DBH Oath of Confidentiality COM027 for Civil action and Sanctions).

A complaint may be filed directly with the Secretary of Health and Human Services for an alleged violation of 42 CFR Part 2.

Listed below are the types of penalties that require sanctions to be applied. They are defined at Tiers 1, 2, 3 and 4 depending on the seriousness of the violation. Please refer to the Federal Register for Tiers:

Penalty Tiers
- https://www.federalregister.gov/d/2019-08530/p-8

Penalty Values
- https://www.federalregister.gov/d/2019-08530/p-11
- https://www.federalregister.gov/d/2019-08530/p-18

Note: On November 15, 2021 the Centers for Medicare & Medicaid Services published the Adjustment of Civil Monetary Penalties for Inflation and the Annual Civil Monetary Penalties Inflation Adjustment for 2021.

References

The Health Information Technology for Economic and Clinical Health (HITECH) Act Section 45 C.F.R. §164.530(e)3402(e)(4) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf

Health Insurance Portability and Accountability Act (HIPAA), Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164

California Board of Behavioral Sciences. Statutes and Regulations Pertaining to the Practice of Professional Clinical Counseling, Marriage and Family Therapy, Educational Psychology, Clinical Social Work. Retrieved December 29, 2021, from: http://www.bbs.ca.gov/pdf/publications/lawsregs.pdf

California Legislative Information. Business and Professions Code 805. Retrieved December 29, 2021 from: http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=805

Continued on next page

Related Policies

DBH Standard Practice Manual and Departmental Forms:

- Confidentiality of Protected Health Information (PHI) (COM0905)
- Privacy Incident Policy (COM0944)
- Code of Conduct (COM003)
- Code of Professional Conduct for Alcohol and Other Drug (AOD) Staff Acknowledgement (SUDRS001)