Confidentiality of Protected Health Information (PHI)

Effective Date	01/03/2007
Revised Date	10/01/2025

DocuSigned by: Dr. Georgina Yoshioka 7DF8077EF4874B2...
Georgina Yoshioka, DSW, LCSW, MBA, Director

Policy

It is the policy of the Department of Behavioral Health (DBH) to adhere to state and federal confidentiality, privacy, and security laws and to apply those laws and regulations which provide the greatest degree of protection and autonomy for clients when providing care, treatment, and in the course of business.

Purpose

To inform DBH staff of State and Federal laws that ensure the confidentiality, privacy, and security of client Protected Health Information (PHI).

Definitions

Business Associate (BA): An entity whom conducts the following on behalf of the covered entity where the provision of services named involves the disclosure of PHI: creates, receives, maintains or transmits PHI for a function or activity involving the use or disclosure of PHI, including claims processing/administration, data analysis, data storage, utilization review, quality assurance, billing, benefit management, practice management, and repricing; provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services.

Covered Entity (CE): A health plan, healthcare clearinghouse, or a healthcare provider who transmits any health information in electronic form in connection with a HIPAA covered transaction.

Designated Record Set: A group of records maintained by or for DBH that consists of the medical records and billing records of a DBH client, record is any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for DBH.

Disclosure: The release, transfer, provision of access to, or divulging in any other manner, of PHI outside the covered entity holding the information.

Health Insurance Portability and Accountability Act (HIPAA): A federal law designed to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Continued on next page

Confidentiality of Protected Health Information (PHI), Continued

Definitions, continued

Information Blocking: A practice that interferes with, prevents, or materially discourages access, exchange, or use of electronic health information. This practice ensures a client's right to access their paper and/or electronic records under existing HIPAA rules, while preventing any unnecessary restrictions by an authorized DBH staff member.

Preemption of State Laws: In cases of perceived conflict among laws and/or regulations, the general rule is that precedence is given to the law and/or rule which provides the greatest protection of client privacy unless disclosure is required by state or federal law. Questions regarding preemption issues may be directed to the DBH Privacy Officer.

Protected Health Information (PHI): Individually Identifiable Health Information (IIHI) held or is transmitted by a covered entity or its business associate, in any form or medium 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.

Use: The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within the covered entity that maintains the information.

Workforce: Employees, volunteers, trainees, students, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Administrative Requirements

DBH, as a covered entity under HIPAA, must adhere to the following administrative requirements:

Requirement	Description
Privacy Officer Designation	The Privacy Officer is responsible for ensuring security safeguards are implemented by the Security Officer, as well as for implementing a privacy program which includes the establishment of the following:

Continued on next page

Confidentiality of Protected Health Information (PHI), Continued

Administrative Requirements, continued

Requirement	Description
Privacy Officer Designation, continued	• Privacy policies and procedures to assure confidentiality of PHI is maintained; • Effective training and education regarding privacy practices; • Investigation of incidents in which a breach of PHI may have occurred; • Breach reporting, in accordance with state and federal laws, and • Ensuring privacy risk assessments are conducted every three (3) years.
Training of Workforce	DBH workforce requirements are as follows: • DBH staff will receive training on privacy, security and confidentiality laws, policies and procedures to the degree necessary and appropriate to carry out their duties and responsibilities regarding safeguarding client PHI. • HIPAA Privacy and Security and Authorization for Release of PHI Training will be completed via the online Learning Management System prior to accessing client PHI but not later than thirty (30) days from commencement of employment, internship, work experience or volunteerism and **annually** thereafter. • Proof of training completion of all required trainings must be maintained in the employee file. Contracted providers must provide documentation of proof of training completion as required by their contract with DBH. • Ongoing education and training will provide staff the ability to remain informed regarding state and federal requirements, and ensure adherence with said requirements, as well as provide quality care and services in a culturally and linguistically competent manner as noted in the Education and Training Policy (TRA8001).

Continued on next page

Confidentiality of Protected Health Information (PHI), Continued

Administrative Requirements, continued

Safeguards	DBH will take reasonable steps to safeguard PHI from intentional or unintentional misuse, regardless of medium (electronic, hard copy, etc.) by implementing and keeping appropriate administrative, technical, and physical safeguards in place to protect the privacy of PHI that includes the following: • Safeguards to ensure DBH clients and visitors cannot view client medical records or files at the counter or reception desk at check-in. • PHI belonging to DBH clients should be restricted to areas where only DBH staff have access including client PHI located on message boards, client schedules, and other postings that are utilized by staff.
Waiver of Rights	DBH cannot require clients to waive their right to file a privacy and/or confidentiality complaint with the Office of Civil Rights, US Department of Health and Human Services, as a condition for treatment, payment, or billing for services provided, nor can DBH require workforce members to waive their rights to file a privacy and/or confidentiality complaint with the Office of Civil Rights, US Department of Health and Human Services as a condition of employment.
Policies and Procedures	DBH will maintain policies and procedures related to privacy and confidentiality of PHI in written or electronic form for six (6) years from the date of creation or the date when they were last in effect, whichever is later (see Security of Protected Electronic Health Information Policy (COM0923) for additional information).

Uses and Disclosures of Protected Health Information (PHI)

The following authorization requirements apply when using and/or disclosing Mental Health and/or SUD PHI.

For…	Then…
Mental Health	The use and/or disclosure of PHI **without** an authorization is allowable under HIPAA for Treatment, Payment and/or health care Operations (TPO).

Continued on next page

Confidentiality of Protected Health Information (PHI), Continued

Uses and Disclosures of Protected Health Information (PHI), continued

For…	Then…
Substance Use Disorder (SUD)	The use and/or disclosure of SUD PHI requires an authorization signed by a client or their legal representative as stipulated in 42 CFR Part 2 of the regulations. Clients may now complete a single Authorization for Release of PHI (COM001) for TPO. A copy of the signed authorization must accompany every disclosure.

Note: For instructions on how and when to complete an authorization form, see Authorization to Release PHI policy (COM0912).

MHP and MCP Data Sharing and Confidentiality

DBH and MCP will ensure the safe sharing of PHI in a timely manner, in accordance with appropriate data sharing, confidentiality and data exchange methods as well as the applicable privacy law(s). If/when signed authorization is required to disclose PHI under 42 C.F.R. Part, HIPAA or WIC 5328, MCP and MHP/DMC-ODS mutually agree to utilize the MHP/DMC-ODS Authorization to Release PHI Form: COM001_E (English); COM001_S (Spanish); COM001_V (Vietnamese) that can be found on the MHP/DMC-ODS website.

DBH will share PHI with MCPs for the purposes of TPO, including care coordination, without need to obtain client Authorization for sharing of mental health PHI; and with a client Authorization for sharing SUD PHI (see Uses and Disclosures of PHI section above).

Minimum Necessary

The minimum necessary standard applies to all disclosures of client PHI and requires reasonable efforts be made to limit PHI disclosed to the minimum information necessary to the fewest number of recipients needed to accomplish the intended purpose.

Minimum necessary does not apply to:

- Disclosures to or requests by a health care provider for TPO, as permitted by and in compliance with federal regulation 45 CFR Section 164.506.

Notice of Privacy Practices

Each client will be provided information in writing, in the threshold language of their preference, about their privacy rights and how their PHI may be used and disclosed. See HIPAA Notice of Privacy Practices (NOPP) Policy (COM0910).

Continued on next page

Confidentiality of Protected Health Information (PHI), Continued

Request for Privacy Protection

Under the HIPAA Privacy Rule, a client may request to restrict the use and disclosure of their PHI, however, DBH is not required to accommodate a client's request if the request interferes with TPO purposes that are often necessary for providing quality patient care and ensuring efficient payment for health care.

If an agreement is made with the client to restrict the disclosure of their PHI, DBH must comply with the agreed restrictions, except for purposes of treating a client in a medical emergency. For example, if a DBH client has a medical emergency, pertinent PHI about the client may be shared between covered entities to provide emergency treatment.

Per 45 CFR 164.522(a)(1)(vi), DBH must comply with a client's request to restrict disclosure of their PHI to a health plan when both of the following conditions are met:

1. The disclosure is for payment or health care operations and **is not** otherwise required by law; and
2. The PHI pertains solely to a health care service for which the client, or a person other than the health plan on behalf of the client, has paid the covered entity in full.

Client Access to PHI

The Cures Act provides clients the right of access to inspect and obtain a copy of their PHI in the designated record set, for as long as the PHI is maintained in the designated record set, and as permitted by law.

The Cures Act prohibits any form of information blocking that interferes with the access, exchange, or use of a client's electronic health information as notated in Health and Safety Code section 123100).

Amendment of PHI

The client has the right to request amendment/correction of PHI in a document in the designated record set. Such requests will be made in writing by completing and submitting a Request To Amend Protected Health Information (COM023_E) to the Medical Records unit.

Accounting of PHI Disclosures

To the extent permitted by law, a client has the right to receive an accounting of PHI disclosures made by DBH in the six years prior to the date on which the accounting is requested, except for the following disclosures:

1. To carry out mental health treatment, payment or billing, and health care operations (SUD records require client written consent and specification of disclosure as required in COM001_E).
2. To the client.
3. Incidental uses or disclosures permitted or required by law.

Continued on next page

Confidentiality of Protected Health Information (PHI), Continued

Accounting of PHI Disclosures, continued

4. Pursuant to an authorization signed by the client or client's representative.
5. To DBH directory, to persons involved in client's care, or for notification purposes.
6. For national security or intelligence purposes.
7. To correctional institutions or law enforcement officials.
8. To the courts or court officials under a Judge's order.
9. Those that occurred prior to the HIPAA compliance date (April 14, 2003)

Note: Clients may request one (1) accounting of disclosures free of charge every twelve (12) months. An additional request of the same accounting of disclosures within a 12-month period (from the initial request), may result in an added fee.

Accounting of PHI Disclosures, continued to Business Associates

DBH may disclose PHI to a business associate and may allow a business associate to create or receive PHI on its behalf if DBH completes a Business Associate Agreement (BAA) with the recipient in advance of data sharing.

Business Associate is held to the same standard as DBH to ensure that PHI is protected and that any breach of unsecured PHI is reported to DBH Compliance in accordance with the written agreement.

Use and Disclosure for Research Purposes

DBH may use or disclose PHI for research provided the research meets all applicable State or Federal laws or regulations. All research requests must be approved in advance by the DBH Institutional Review Board (IRB). If the research is not authorized by the subject client, the PHI must be de-identified by redacting all identifiers on all documents in accordance with the Department of Health Care Services (DHCS) HIPAA Identifiers List.

Related Policies, Procedures, and Forms

DBH Standard Practice Manual and Forms:

- Sending Confidential Information by Facsimile Policy (COM0901)
- Unauthorized Access of Confidential Medical Records (COM0907)
- Electronic Transfer of Client Protected Health Information – Internet and Intranet Policy (COM0909)
- HIPAA Notice of Privacy Practices (NOPP) Policy (COM0910)
- Authorization to Release PHI Policy (COM0912)
- Security Of Protected Electronic Health Information Policy (COM0923)
- Data Integrity Policy (COM0925)
- HIPAA Violation Sanctions Policy (COM0926)
- Medi-Cal Eligibility Data System (MEDS) Policy (COM0943)
- Privacy Incident Policy (COM0944)

Continued on next page

Confidentiality of Protected Health Information (PHI), Continued

Related Policies, Procedures, and Forms, continued

- 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)
- Workstation and System Security Policy (IT5022)
- Education and Training Policy (TRA8001)
- Health Insurance Portability and Accountability (HIPAA) (14-03)
- Patient Privacy Rights (14-03 SP 07)

San Bernardino County Policy Manual:

- Non-Public Personally Identifiable Information (14-02)
- Health Insurance Portability and Accountability (HIPAA) (14-03)
- Patient Privacy Rights (14-03 SP 07)

References

- 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.
- California Health & Safety Code, Section 123100 et seq. (Patient Access to Health Records)
- California Welfare and Institution Code, Section 5328 et seq. (Lanterman-Petris-Short Act)
- Department of Health Care Services (DHCS), List of HIPAA Identifiers
- Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, Privacy Rule (HIPAA)
- HIPAA Administrative Simplification, 45 CFR Parts 160, 162, and 164 (Standard: Minimum necessary)
- HIPAA, Privacy, and Security Training, DBH Relias Learning
- Title 42 of the Code of Federal Regulations CFR, Section 2.1 et seq.
- Title 45 CFR Section 45 CFR 164.522(a)(1)(vi), Rights to request privacy protection for protected health information.
- Title 45 CFR Section 164.528, Public Welfare, Accounting of disclosures of protected health information.