City and County of San Francisco
Daniel Lurie, Mayor

San Francisco Department of Public Health
Daniel Tsai
Director of Health

San Francisco Department of Public Health

*Policy & Procedure Detail**

Policy & Procedure Title: A.1.0 DPH Privacy Policy	
Category: Privacy	
Effective Date: 3/2003	**Last Reviewed/Revised:** 2/19/2026
DPH Unit of Origin: Office of Compliance and Privacy Affairs	
Policy Contact - Employee Name and Title; and/or DPH Division: Office of Compliance and Privacy Affairs (OCPA)	
Contact Phone Number(s): (855) 729-6040	
Distribution: DPH-wide X	**If not DPH-wide, other distribution:**

All sections in table required.

I. **Purpose and Scope:**

A. **Purpose:** The purpose of this policy is to provide guidance to providers, San Francisco Department of Public Health ("DPH") employees, UCSF affiliate staff, Community Based Organizations with DPH contracts (CBOs) staff, other DPH contractors, students, and volunteers (collectively referred to as "workforce members") by setting forth the basic requirements for protecting the confidentiality of patient medical information. It provides an overview of the Health Insurance Portability and Accountability Act (HIPAA), other Federal privacy and security regulations, and State healthcare privacy and security regulations.

It is the policy of DPH to comply with HIPAA, HITECH Act, 42 CFR Part 2, and other Federal privacy regulations and State healthcare privacy regulations. Each division and unit shall ensure that its policies and procedures are consistent with this department-wide policy and procedure.

B. **Scope:** This policy pertains to all workforce members who access, use, or disclose DPH patient protected health information (PHI). The policy is administered by the Office of Compliance and Privacy Affairs (OCPA). It is intended to serve as a foundation for DPH privacy practices.

This policy provides an overview of the requirements of HIPAA and other key privacy policies. There are more detailed DPH policies regarding these topics, which can be found on the DPH Privacy Policies website.

II. **HIPAA:**

A. **Background:** The Health Insurance Portability and Accountability Act (HIPAA} was established to protect the privacy of individuals receiving health care services. HIPAA establishes a national standard for the minimum level of protection for medical information

through the part of HIPAA referred to as the Privacy Rule.

B. **Privacy Rule:** The HIPAA Privacy Rule protects all “individually identifiable health information” held or transmitted by a covered entity in any form or media, whether electronic, paper, or oral. The HIPAA Privacy Rule calls this information "Protected Health Information" or "PHI." PHI is information relating to an individual’s health, the care received, and/or payment for services plus patient identifying data. See Appendix A for a list of patient identifiers.

C. **PHI:** PHI is information, including demographic data, that relates to:

1. An individual’s past, present, or future physical or mental health or condition.
2. The provision of health care to the individual.
3. The past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe the information can be used to identify the individual. Individually identifiable health information includes many common identifiers such as name, address, date of birth, and Social Security number.

D. **Examples of PHI:** PHI includes a medical record, claim or bill, assessment form, and sign-in sheet for a group therapy session.

E. **Treatment, Payment, Operations (TPO) Disclosures:** The basic principle of the Privacy Rule is that providers may use and disclose PHI without an individual’s authorization only for treatment, payment, and health care operations. Other uses and disclosures of PHI generally require the written authorization of the individual.

F. **Minimum Necessary:** The Privacy Rule also includes the concept of "minimum necessary." This requirement mandates that when using or disclosing PHI, or when requesting PHI from external providers or entities, providers will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose. The Privacy Rule does recognize that providers may need to use an individual’s health information in the provision of patient care and/or public health purposes. However, access to PHI by workforce members must be limited based on job scope and the need for the information.

G. **Patient Rights:** The Privacy Rule includes a set of rights for consumers of health care services. Examples include the right to: obtain a written notice explaining how DPH will use and disclose their information, access and receive copies of their health information, and request that information be communicated in particular ways to protect confidentiality.

H. **Security Rule:** Another section of HIPAA contains the Security Rule. The Security Rule focuses on ensuring that protected health information in an electronic format (ePHI) remains secure, while allowing covered entities to adopt new technologies to improve quality and efficiency of patient care. Examples of ePHI are the electronic medical record, datasets from DPH systems which contain PHI and any PHI sent electronically such as via email. Several DPH IT policies address security issues.

III. **California Confidentiality of Medical Information Act (CMIA):**

A. **CMIA**: California also has a privacy statute known as the California Confidentiality of Medical Information Act (CMIA). CMIA defines who may release confidential medical information and under what circumstances. CMIA prohibits the sharing, selling, or otherwise unlawful use of medical information. CMIA also imposes requirements on the written authorization used for disclosure of medical information. The Lanterman- Petris-Short Act ("LPS Act") applies to Psychiatric Emergency Services (PES), and inpatient psychiatry.

Further, other Federal and State statutes provide additional protection for medical, behavioral health, and substance use disorder information in situations where laws conflict or overlap, DPH must comply with the law that provides the patient with the greatest protection. Determining which law applies can be complex. Any questions should be referred to OCPA.

IV. **Use and Disclosure of PHI for Treatment, Payment, and Health Care Operations (TPO):**

A. **Permitted TPO Uses:** Workforce members may use PHI for TPO without an individual's authorization. TPO is defined as follows:

1. **Treatment:** means providing, coordinating, or managing a patient's care and related services among health care providers. Treatment includes patient education and training, as well as consultations between providers and referrals.
2. **Payment:** means activities related to being paid for services rendered. Payment encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

   In addition to the general definition, common examples of payment activities include, but are not limited to, the following:

   i. Determining eligibility or coverage under a plan and adjudicating claims;

   ii. Risk adjustments;

   iii. Billing and collection activities;

   iv. Reviewing health care services for medical necessity, coverage, justification of charges, and eligibility determinations;

   v. Utilization review activities; and

   vi. Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about the covered entity).

3. **Health care operations** are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. These activities, which are limited to the activities listed in the definition of "health care operations" at 45 CFR 164.501, include:

    i. Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;

    ii. Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;

    iii. Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims;

    iv. Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;

    v. Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and

    vi. Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

B. **Minimum Necessary Uses and Disclosures:**

1. **Requirement:** When using or disclosing PHI, or when requesting PHI from a non-DPH provider or entity, DPH providers and staff shall make reasonable efforts to limit the PHI requested, used, or disclosed to the minimum necessary to accomplish the patient's care.
2. **Job Scope/Duties:** DPH shall identify those in its workforce who need access to PHI and limit access based on job scope and the need for the information. This includes limiting access in the Electronic Health Record (EHR).
3. **Exceptions:** The *minimum necessary* requirement does not apply to the following:

    i. Disclosures to, or requests by, a DPH health care provider for treatment purposes;

ii. Uses or disclosures made to the individual who is the subject of the information;

iii. Uses or disclosures made pursuant to the individual's authorization;

iv. Disclosures made to the Secretary of the Department of Health and Human Services when disclosure is required for enforcement purposes; and

v. Other uses or disclosures such as those required by law, made pursuant to a subpoena or court order for workers' compensation purposes.

C. **Special Requirements for Behavioral Health Information, Substance Use Disorder Information, and Health Information of Minors:**

1. **Behavioral Health Information: Although** the Privacy Rule largely does not make a distinction between medical and behavioral health information, California state law provides for special protections for behavioral health information. CMIA addresses the confidentiality of behavioral health information.

2. **Permitted Disclosures:** Behavioral health information may be shared with medical and behavioral health providers treating the same patient (client) even if they are not part of the SFHN or a contracted provider (e.g. emergency room staff at another hospital or a psychiatrist). Other uses and disclosures may require the specific authorization of the patient to disclose behavioral health information. Behavioral health information includes progress notes[1], medication prescription and monitoring, results of clinical tests, treatment plans, symptoms and prognosis recorded by behavioral health professionals.

3. **LPS Act**: The Lanterman-Petris-Short Act ("LPS Act") applies to Psychiatric Emergency Services (PES), and inpatient psychiatry. The confidentiality provision of LPS (section 5328 of CA Welfare and Institutions Code) states that "all information and records obtained in the course of providing services under [specific divisions of LPS] to either voluntary or involuntary recipients of services shall be confidential."

   Some of the provisions in LPS differ from those in HIPAA as it allows for additional permitted disclosures as well as other additional restrictions on the use and disclosure of PHI.

4. **Substance Use Disorder Information:** Information pertaining to substance use disorder clients in designated substance use disorder programs is subject to special protection under Federal statute 42C.F.R. part 2. Additionally, California Health and Safety Code Section 11977 provides special protections for information of certain substance use disorder programs.

   Substance use disorder information obtained outside of a 42 CFR Part 2 program is not subject to these provisions. Therefore, substance use disorder information obtained under those situations may be shared among DPH providers and to its contracted providers without authorization of the patient for patient care purposes.

5. **HIV Test Results:** Per state law, DPH cannot disclose HIV test results without specific, written authorization from the patient, except for purposes of diagnosis, care, or treatment of the patient by DPH providers.

6. **Minors:** Use and disclosure of protected health information associated with the care of minors should be administered using the same principles as consent for treatment. If the minor can consent for services per Federal or State statute or DPH policy, then the minor controls his or her privacy rights.

D. **Disclosures to Family, Other Relatives, Close Personal Friends, and Personal Representatives:**

1. **Involved in Patient's Care**: DPH providers may disclose only the information that the person involved needs to know about the individual's care or payment for care to an individual's family members or other relatives, close personal friends, or any other person identified by the individual when the individual agrees verbally or in writing, there is no objection when the individual is provided with an opportunity to object; or if the treating provider determines in their professional judgement when the patient cannot make a decision.
2. **Incapacitated:** If the individual is not present or is incapacitated, the provider may disclose information to family members, relatives, or close friends if the provider believes disclosure is in the best interest of the individual.
3. **Substance Use Information:** Generally, no information may be disclosed to a family member, relative, or close friend regarding behavioral health or substance use disorder without the individual's specific authorization.
4. **Personal Representatives:** DPH providers shall disclose information to an individual's personal representative (i.e., those granted legal authority to make health care decisions on behalf of that individual) in the same manner as they would for the individual.

V. **Prohibitions – Unauthorized Access to PHI:**

A. **Unauthorized Access:** Access or looking at PHI without having a permitted and legitimate business purpose is against the law. This includes accessing your own medical record maintained by DPH. DPH may restrict, suspend, or permanently revoke a user's access to any DPH PHI, confidential information, and/or data systems, initiate and/or recommend disciplinary action (including termination), and, if applicable, report a user to regulatory bodies including professional boards.

B. **Enforcement**

1. **Responsibility:** Each DPH workforce member is responsible for understanding and complying with this policy and HIPAA.
2. **Training:** Each DPH workforce member is required to complete the annual compliance and privacy training every calendar year, which includes verifying agreement and compliance with the DPH User Agreement for Confidentiality, Data Security, and Electronic Signature. In addition, every calendar year, each DPH workforce member is required to acknowledge that they have read and understand the standards included in the DPH Code of Conduct and agree to comply fully with these standards.
3. **Managers and Supervisors:** It is the responsibility of DPH managers and supervisors to ensure that their direct reports complete the compliance and privacy training that is provided to all workforce members on an annual basis and that workforce members reporting to them are complying with DPH privacy policies. DPH managers

and supervisors are also responsible for confirming on an annual basis that their direct reports have signed the DPH User Agreement for Confidentiality, Data Security, and Electronic Signature and acknowledgement of Code of Conduct.

4. **Sanctions:** DPH has and will apply appropriate sanctions against any DPH workforce member who fails to comply with DPH Privacy policies and procedures. The workforce member's manager and/or Human Resources will document any sanctions applied.
5. **Reporting:** Any DPH workforce member who knows of, suspects, or has a question regarding a possible violation of HIPAA shall contact OCPA. No workforce member shall be retaliated against for reporting a possible violation. If the workforce member wishes to remain anonymous, that workforce member may call the DPH Privacy and Compliance Hotline at (855) 729-6040 or email compliance.privacy@sfdph.org.
6. **Discipline:** DPH workforce members who violate HIPAA and other privacy regulations may be disciplined through the civil service process, up to and including termination, and in accordance with any applicable Memorandum of Understanding.
7. **OCR Enforcement:** The Federal Office for Civil Rights ("OCR") of the Department of Health and Human Services will enforce HIPAA on behalf of the Federal government. Workforce members may file a complaint with the OCR and are not required to use the DPH complaint process.
8. **Penalties:** There are both civil monetary penalties and criminal sanctions for violations of HIPAA and CMIA, and other federal and state privacy and security rules.
9. **Criminal Sanctions:** Criminal sanctions, including larger fines and imprisonment, may be imposed for knowingly disclosing or obtaining PHI in violation of HIPAA.

Appendix A
HIPAA 18 Patient Identifiers

HIPAA specifies 18 elements in health data that are considered patient identifiers. If any are present, the health information is considered PHI and **cannot** be released without patient authorization.

• Name	• Social Security Number (SSN)
• Postal Address	• Account numbers
• All elements of dates, except year	• License numbers
• Telephone numbers	• Health plan beneficiary numbers
• Fax numbers	• Device identifier and their serial numbers
• Email address	• Vehicle identifiers and serial numbers
• URL address	• Biometric identifier (including finger and voice prints)
• IP address	• Full face photo and other comparable images
• Medical record number	• Any other unique identifying number, code or characteristic

Last Reviewed: 5/31/2023; 2/19/2026