



City and County of San Francisco
London N. Breed, Mayor

San Francisco Department of Public Health

Grant Colfax, MD 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: 5/31/2023
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.*

1. Purpose of Policy

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 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.

2. Policy

STATEMENT OF POLICY

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.

SCOPE

This policy pertains to all individuals who may access, use, or disclose DPH patient protected health information (PHI); this policy will refer to these individuals as “DPH employees.” 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.

BACKGROUND

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. The intent

The mission of the San Francisco Department of Public Health is to protect and promote the health of all San Franciscans.

We shall ~ Assess and research the health of the community ~ Develop and enforce health policy ~ Prevent disease and injury ~
~ Educate the public and train health care providers ~ Provide quality, comprehensive, culturally-proficient health services ~ Ensure equal access to all ~

of the statute and the regulatory rule is to expand consumer control over their medical information. 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.

PHI 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 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.

Examples of PHI include a medical record, claim or bill, assessment form, and sign-in sheet for a group therapy session. The basic tenet of HIPAA is that providers may use and disclose PHI without the individual’s authorization only for treatment, payment, and health care operations. A patient’s authorization is not required for certain public interest related purposes such as public health reporting. Other uses and disclosures of PHI generally require the written authorization of the individual.

HIPAA 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. HIPAA 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 the workforce must be limited based on job scope and the need for the information.

HIPAA 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.

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.

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.

COMPARISON WITH EXISTING STATE LAWS

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.

3. Procedures

I. Use and Disclosure of PHI for Treatment, Payment, and Health Care Operations

1. DPH employees, affiliates, and contract providers may use PHI for treatment, payment, and health care operations without an individual's authorization.
2. Treatment, payment, and health care operations are 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:

- Determining eligibility or coverage under a plan and adjudicating claims;
 - Risk adjustments;
 - Billing and collection activities;
 - Reviewing health care services for medical necessity, coverage, justification of charges, and eligibility determinations;
 - Utilization review activities; and
 - 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:

- Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;
- 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;
- 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;
- Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
- 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.

Looking at patient information without having a permitted and legitimate business purpose is against the law; DPH may restrict, suspend, or permanently revoke a user's access to any SF DPH 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.

II. Minimum Necessary Uses and Disclosures

1. 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. 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. The *minimum necessary* requirement does not apply to the following:
 - e. Disclosures to, or requests by, a DPH health care provider for treatment purposes;
 - f. Uses or disclosures made to the individual who is the subject of the information;
 - g. Uses or disclosures made pursuant to the individual's authorization;
 - h. Disclosures made to the Secretary of the Department of Health and Human Services when disclosure is required for enforcement purposes; and

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

III. Special Requirements for Behavioral Health Information, Substance Use Disorder Information, and Health Information of Minors

a. Behavioral Health Information

1. CMIA

Although the Federal HIPAA 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. 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 notes¹, medication prescription and monitoring, results of clinical tests, treatment plans, symptoms and prognosis recorded by behavioral health professionals.

2. 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.

- (a) Disclosures required by LPS;
- (b) Disclosures permitted with authorization include, but are not limited to, the following:
 - Disclosure to Professionals not employed by facility who do not have responsibility for patient's care;
 - Disclosure authorized by a patient representative;
 - Disclosure for life/disability insurance;
 - Disclosure to patient's attorney;
 - Disclosure to probation officer;
 - Disclosure to employer;

¹ DPH policy prohibits the use of psychotherapy notes. [DPH BHS policy: Restrictions of Psychotherapy Notes and Informal Memory Prompts]

(c) Disclosures permitted without patient authorization:

- Statutory exceptions – including, but not limited to treatment; payment; conservatorship proceedings; coroner; county social worker, probation officer, foster care public health nurse or others caring for minor; research; disclosure to US HHS.
- Disclosures to law enforcement officials
 - Protection of elected officials
 - Crime on the premises
 - Reporting movement and identification information to the CA Department of Justice (DOJ)
 - Disappearance of ‘holdable’ voluntary patient
 - Disappearance or transfer of criminal defendant determined to be mentally incompetent to stand trial
 - Crime investigation
 - Escape from state mental health facility
 - Escape of involuntary mental health patient
 - Release of patient after 72-hour old who is under criminal investigation
 - Law enforcement officer with a warrant
 - Correctional agencies
- Disclosures to various state governmental entities
 - CA Department of Public Health (CDPH) and CA Department of Social Services (CDSS)
 - Professional licensing boards – when the Director of State Hospitals has reasonable cause to believe there has been a violation of law subject to the jurisdiction of such board, or made pursuant to other provisions of law.
 - Reports of firearm possession prohibition to the CA DOJ
- Disclosures to EMSA, LEMSAs, and EMS providers for minimally necessary and specific data elements for quality assessment and improvement purposes.
- Disclosures regarding protection of individuals
 - Including, but not limited to: patient presents serious threat of violence; mandated reporting in general; multidisciplinary personnel teams; death review teams; Ryan White CARE Act: Emergency; Response Employee-Designated Officer.
- Disclosure of Information to Courts
- Response to Subpoena that Requests LPS Records

(d) Disclosure about Inpatients to family and others

- HIPAA contains a broad provision permitted disclosure of PHI to persons involved in the individual's care and for notification purposes. This provision is not applicable for these LPS cases and LPS rules must be followed.
- Notifying next of Kin and others of the Patient's Admission
 1. The patient must be advised by the facility that he or she has the right to request that this information not be provided. Documentation of this advisement and the patient's instruction should be placed in the medical record.
 2. If the patient arrives in the emergency department unconscious or otherwise unable to communicate, a general acute care hospital must attempt to contact the patient's agent, surrogate, family member or other person the hospital reasonably believes has the authority to make health care decisions on behalf of the patient.
- Notifying Next of Kin and Others of the Patient's Release, Transfer, Illness or Death
 1. The hospital must make reasonable attempts to notify a patient's next of kin or other person designated by the patient of the patient's release, transfer, serious illness, injury, or death, upon the request of the family member, unless the patient asks that this information not be provided.
 2. The hospital also must inform the patient of the right to request that this information not be disclosed. Documentation of this advisement and of the patient's instructions should be placed in the patient's record.
- Notifying family members and others of the Patient's Condition
 1. Upon request of a family member of a patient (or other person designated by the patient), a facility must give the family member (or the designee) notification of the patient's diagnosis, the prognosis, the medications prescribed, the side effects of medications prescribed, if any, and the progress of the patient, if, after notification of the patient that this information is requested, the patient authorizes its disclosure.
 2. The patient's written authorization should be obtained. If the patient is unable to authorize the release of this information, notation of the attempt to get the patient's authorization must be made in the patient's medical record and daily efforts must be made to secure the patient's authorization or refusal.
 3. However, if a request for information is made by the spouse, parent, child or sibling of the patient and the patient is unable to authorize the release of such information, the requestor must be given

notification of the patient's presence in the facility, except to the extent prohibited by federal law.

(e) Disclosures to Mental Health Advocacy programs

- Investigations by the Disability Rights California (DRC). DRC must be given reasonable unaccompanied access to public or private facilities, programs, and services, and to recipients of services therein, at all times necessary to investigate incidents of abuse and neglect.
- DRC must be given reasonable unaccompanied access to public or private facilities, programs and services, and to recipients of services therein, during normal working hours and visiting hours for other advocacy services.

Questions regarding the use or disclosure of behavioral health information should be referred to OCPA.

b. Substance Use Disorder Information

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

c. 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.

d. 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.

IV. Disclosures to Family, Other Relatives, Close Personal Friends, and Personal Representatives

- a. 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:
 1. upon the individual's oral agreement;
 2. if there is no objection when the individual is provided with an opportunity to object; or

3. if the treating provider determines in their professional judgement when the patient cannot make a decision.

Note that minor consent rules apply if treatment is provided as described in section III.d above. If oral agreement is obtained or no objection is raised, this must be recorded in the patient's medical record.

- b. 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.
- c. 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. This applies also to minors who consent to treatment or otherwise control their PHI under minor consent rules discussed in section III.d above.
- d. 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. Enforcement

- a. Each DPH employee is responsible for understanding and complying with this policy and HIPAA.
- b. Each DPH employee 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 employee 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.
- c. It is the responsibility of DPH managers and supervisors to ensure that their employees complete the compliance and privacy training that is provided to all employees on an annual basis and that employees reporting to them are complying with DPH privacy policies. DPH managers and supervisors are also responsible to confirm on an annual basis that their employees have signed the DPH User Agreement for Confidentiality, Data Security, and Electronic Signature and acknowledgement of Code of Conduct.
- d. DPH has and will apply appropriate sanctions against any DPH employee who fails to comply with DPH Privacy policies and procedures. The employee's manager and/or Human Resources will document any sanctions applied.
- e. Any DPH employee who knows of, suspects, or has a question regarding a possible violation of HIPAA shall contact OCPA. No employee shall be retaliated against for reporting a possible violation. If the employee wishes to remain anonymous, that employee may call the DPH Privacy and Compliance Hotline at (855) 729-6040 or email compliance.privacy@sfdph.org.
- f. DPH employees 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.

- g. The Federal Office for Civil Rights ("OCR") of the Department of Health and Human Services will enforce HIPAA on behalf of the Federal government. DPH employees, patients, and clients may file a complaint with the OCR and are not required to use the DPH complaint process.
- h. There are both civil monetary penalties and criminal sanctions for violations of HIPAA and CMIA, and other federal and state privacy and security rules.
- i. Criminal sanctions, including larger fines and imprisonment, may be imposed for knowingly disclosing or obtaining PHI in violation of HIPAA.

4. References

- a. Questions about the information contained in this policy should be directed to the DPH **Office of Compliance and Privacy Affairs**.
 - i. DPH Compliance and Privacy Toll-Free Hotline: 855-729-6040
 - ii. DPH Compliance and Privacy Office: compliance.privacy@sfdph.org
 - iii. DPH Compliance website: sf.gov/OCPA
- b. DPH Policy "HIPAA Compliance: Authorization for Use and Disclosure of Protected Health Information"
- c. DPH policy "HIPAA Compliance: Administrative Requirements"
- d. DPH Code of Conduct

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