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 Reissue/Revision Date:** 10/18/2021
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, other San Francisco Department of Public Health ("DPH") employees, UCSF affiliate staff, CBO staff, 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 regulations and State healthcare privacy 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 at DPH, and others who may access, use, or disclose DPH patient 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.

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

HIPAA uses the term "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 identifying data. PHI includes patient identifying data **plus** information about:

- 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,

It includes all information related to the individual's health care whether verbal, written, or in electronic format that can be identified as belonging to a particular person. 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 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 here.

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. 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). 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

A. DPH employees, affiliates, and contract providers may use PHI for treatment, payment and health care operations.

B. Treatment, payment and health care operations are defined as follows:

1. **Treatment** means providing, coordinating, or managing a patient's care, including patient education and training, consultations between providers and referrals.
2. **Payment** means activities related to being paid for services rendered. These activities include eligibility determinations, billing, claims management, utilization review, and debt collection.
3. **Health care operations** means a broad range of activities such as quality assessment, student training, contracting for health care services, medical review, auditing functions, licensing and accreditation, and general administrative activities.

II. Minimum Necessary Uses and Disclosures

A. 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.

B. 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).

C. The *minimum necessary* requirement does not apply to the following:

1. Disclosures to, or requests by, a DPH health care provider for treatment purposes;
2. Uses or disclosures made to the individual treated, as permitted or required by law;
3. Uses or disclosures made pursuant to the individual's authorization;
4. Disclosures made to the Secretary of the Department of Health and Human Services pursuant to an investigation or compliance review; and
5. 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 Substance Use Disorder and Health Information of Minors

A. **Behavioral Health Information**

1. Although the Federal privacy rule largely does not make a distinction between medical and behavioral health information, California state law does provide special protections for behavioral health information. However, 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

[1] DPH policy prohibits the use of psychotherapy notes. [Site BHS policy on this]

clinical tests, treatment plans, symptoms and prognosis recorded by behavioral health professionals.

2. The CMIA is the state law that addresses the confidentiality of behavioral health information, The Lanterman-Petris-Short Act ("LPS Act") applies to Psychiatric Emergency Services (PES), and inpatient psychiatry. 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 in the course of general medical treatment 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 PHI 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; and
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. Such disclosures shall be limited to information directly relevant to that person's involvement with the individual's care or payment for that care.

C. 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.

D. 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 consenting to treatment under minor consent rules discussed in section III D above.

E. 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 another) in the same manner as they would for the individual.

V. Enforcement (See DPH policy "HIPAA Compliance: Administrative Requirements.")

A. Each DPH employee is responsible for understanding and complying with this policy and HIPAA. It is the responsibility of DPH managers and supervisors to ensure that their employees complete the privacy training that is provided to all employees on an annual basis and that employees reporting to them are complying with DPH privacy policies.

B. Any DPH employee who knows of, suspects, or has a question regarding a possible violation of HIPAA may 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.

C. DPH employees who violate HIPAA and other privacy regulations may be disciplined through the civil service process and in accordance with the applicable Memorandum of Understanding. Discipline may involve actions up to and including termination of employment.

D. 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.

E. There are both civil monetary penalties and criminal sanctions for violations of HIPAA.

F. Criminal sanctions, including larger fines and imprisonment, may be imposed for knowingly disclosing or obtaining PHI in violation of HIPAA.

Contact information for Office of Compliance and Privacy Affairs:

Toll-free Compliance, Ethics and Privacy Hotline: 855-729-6040

Email: Compliance.privacy@sfdph.org

4. References

1. DPH Policy "HIPAA Compliance: Authorization for Use and Disclosure of Protected Health Information"

2. DPH policy "HIPAA Compliance: Administrative Requirements"

Appendix A
HIPAA 18 Patient Individually Identifiable Information

· 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 (finger and voice prints)
· IP address	· Full face photo and other comparable images
· Medical record number	· Any other unique identifying number, code or characteristic