



City and County of San Francisco
London 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.2.0 HIPAA Administrative Requirements	
Category: Privacy	
Effective Date: 11/1/2012	Last Reviewed/Revised Date: 10/18/2021
DPH Unit of Origin: Office of Compliance & Privacy Affairs	
Policy Contact - Employee Name and Title; and/or DPH Division: Office of Compliance & Privacy Affairs (OCPA)	
Contact Phone Number(s): (855) 729-6040	
Distribution: DPH-wide <input checked="" type="checkbox"/>	If not DPH-wide, other distribution:

**All sections in table required. Updated 3/2014*

1. Purpose of Policy

Department of Public Health (DPH) policies are to be followed by all workforce members. This policy outlines requirements necessary to secure Protected Health Information (PHI) in accordance with the Health Insurance Portability and Accountability Act (HIPAA)

The purpose of this administrative policy is to provide DPH workforce members with general administrative policies and procedures that, (in accordance with the HIPAA Privacy Rule), help secure the privacy of health information and protect the privacy rights of individuals who have entrusted their PHI to DPH.

2. Policy

It is the policy of DPH to adopt policies and procedures that fulfill the administrative requirements set forth in HIPAA.

3. Procedures

HIPAA requires DPH to adopt and implement administrative policies and procedures designed to secure the privacy of PHI, and protect the privacy rights of individuals who have entrusted their PHI to DPH.

I. Personnel Assignments

- A. The Director of the Office of Compliance and Privacy Affairs (OCPA)/Chief Integrity Officer is the privacy official responsible for developing and implementing policies and procedures regarding HIPAA as well as other Federal and State privacy policies.

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 ~

- B. OCPA (under the direction of the Director of OCPA) is responsible for receiving complaints from individuals who believe that DPH has violated Federal, or State laws governing PHI and confidential patient information.
- C. This administrative policy documents DPH designated personnel roles and responsibilities.

II. Training

A. Responsibility

1. Department of Public Health (DPH)

- a. It is the responsibility of DPH, through the Director of OCPA, to provide annual privacy training to all DPH personnel, affiliates, contractors, and volunteers who produce, transcribe, store, transmit, or otherwise have access to PHI. The training of new employees and annual training of existing employees shall consist of but not be limited to:
 - (a) On-line specialized healthcare privacy training where accessible,
 - (b) In-service specialized healthcare privacy training where on-line training is unavailable, or
 - (c) Printed, electronic, and in service consulting resources made available through OCPA.
- b. Any material changes in HIPAA, Federal, or State healthcare privacy laws will be incorporated in the annual training. If more immediate action is required, an all-staff memo will be sent to train employees on new material regulatory requirements.

OCPA may require privacy training of staff as part of a corrective action plan for a privacy incident or breach.

2. Department Managers and Supervisors

- (a) Department managers are responsible for verifying that their staff have completed healthcare privacy training sufficiently to perform their duties in compliance with healthcare privacy regulations and policies and procedures.
- (b) Department managers and supervisors are responsible for providing and/or requesting specialized health information privacy training for personnel who report to them.
- (c) Department managers and supervisors are responsible for identifying and notifying OCPA of any unmet healthcare privacy requirements within their departments.

3. DPH Personnel

- a. DPH personnel are responsible for taking healthcare privacy training as new workforce members, annual privacy training for workforce members, and any specialized healthcare privacy training brought to their attention by DPH managers or supervisors;
- b. DPH personnel are responsible for notifying their managers or supervisors of any unmet specialized healthcare privacy training needs that come to their attention.

B. Training Documentation

1. The on-line (electronic) training systems have documentation of privacy training records including signing of the User Agreement for Confidentiality, Data Security and Electronic Signature.
2. These training records will be available for at least six (6) years.

III. Complaints to DPH**A. Policy**

1. DPH shall establish and maintain a process for individuals to register complaints regarding possible healthcare privacy violations, its privacy policies and procedures, and/or its compliance with those policies and procedures. Individuals may contact their site Privacy Officer, email the Office of Compliance and Privacy Affairs at compliance.privacy@sfdph.org or call the DPH Compliance and Privacy Hotline at (855) 729-6040. Individuals may report their concerns anonymously.
2. OCPA shall document all complaints received regarding management of PHI, and document the disposition of those complaints. Documentation shall be retained as required by law.
3. DPH workforce members shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who files a complaint with DPH or with the Department of Health and Human Services.

B. Complaint Process

1. DPH's Notice of Privacy Practices shall direct individuals to submit a complaint regarding management of PHI to their care site or OCPA. The Notice also indicates that a complaint can be made directly to the Secretary of Health and Human Services (HHS).
2. The site Privacy Officer shall receive and review all complaints regarding the management of an individual's protected health information.
3. Disposition of Complaint

No Action Taken. If the review determines that the complaint is without merit, no action will be taken. This disposition shall be noted on the complaint form, and the client so informed.

Further Investigation Required. If the site Privacy Officer determines that a breach of policy or procedure has occurred or that the complaint identifies a potential for process improvement, the individual shall be notified that further review of the complaint is required, and a final disposition will be delivered later. The site Privacy Officer shall refer the complaint to the appropriate department for follow-up (e.g. site management to modify a process or for possible disciplinary action). When the investigation has been completed and the matter resolved, the investigating Privacy Officer shall notify the individual. If a breach of policy or procedure has resulted in an unauthorized use or disclosure of PHI, the site Privacy Officer shall immediately implement steps to mitigate any potential harm to the individual.

4. All complaints to DPH regarding DPH management of PHI and documentation of the disposition of those complaints shall be filed electronically by the site Privacy Officer in a manner conducive to retrieval for review and/or audit. The documentation shall be retained for a period of six years from the date of the complaint.

IV. Policies and Procedures

- A. OCPA shall develop, implement and enforce policies and procedures consistent with HIPAA, as well as applicable Federal and State privacy policies. The policies and procedures will be reasonably designed and take into account the size and type of activities related to protected health information undertaken by DPH.
- B. When necessary, OCPA will revise these policies and procedures and update its training program to reflect applicable changes in HIPAA, Federal, and State law.
- C. If the changes in law materially affects the contents of the Notice of Privacy Practices, OCPA will promptly make the appropriate revisions to the Notice. The revised policy and procedures (due to changes in the law) will not be implemented prior to the effective date of the revised Notice. The revised Notice of Privacy Practices will be posted and made available to patients.
- D. OCPA may change, at any time, a policy or procedure that does not materially affect the Notice.
- E. All policies and procedures (including revisions) will be documented and filed with the Office of Compliance and Privacy Affairs. All action, activity, or designation required by HIPAA, Federal and State laws should be documented and filed with OCPA. The documents will be maintained in electronic format in the OCPA shared drive on the DPH network for a period of at least six (6) years after the creation date.

V. Administrative Safeguards to Protect PHI

- A. The Director of OCPA shall work collaboratively with the Chief Information Officer and Chief Information Security Officer to insure that proper safeguards are in place to insure the use, access and disclosure of PHI is consistent with HIPAA, Federal and State regulations
- B. These safeguards shall include (but are not limited to) effective review and audit protocols to monitor individual, use, access and disclosure of PHI maintained in any form across DPH.
- C. The Director of OCPA shall be responsible for overseeing routine audits of the electronic health record and periodic site audits, to monitor inappropriate use, access, or disclosure of PHI.

VI. Sanctions

- A. DPH has and will apply appropriate sanctions against members of the DPH workforce who fail to comply with DPH privacy policies and procedures, and the requirements of this Administrative Requirements policy. The employee's manager and/or human resources will document any sanctions applied.

VII. Mitigation

- A. OCPA will mitigate to the extent practicable, any harmful effect (that is known) of a use or disclosure of PHI in violation of DPH policies and procedure and the requirements of this Administrative Requirements policy.

VIII. Waiver of Rights

- A. DPH may not require individuals to waive their rights under 45 CFR §160.306 as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

4. References

HIPAA Administrative Requirements: 45 CFR § 164.530

Last Reviewed/Revised Date: 10/18/2021