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: B.1.1 Reporting of Unlawful or Unauthorized Access of Protected Health Information (PHI)	
Category: Privacy	
Effective Date: 9/10/2009	**Last Reviewed/Revised Date:** 2/19/2026
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 ☒	**If not DPH-wide, other distribution:**

I. Purpose and Scope:

A. **Purpose:** The purpose of this policy is to define the responsibilities of the San Francisco Department of Public Health (DPH) in responding to a potential or actual privacy breach of patients' Protected Health Information (PHI) or Personally Identifiable Information (PII). This document establishes guidance for the reporting and investigation of the breach of PHI per the 1996 Health Insurance Portability and Accountability Act (HIPAA), 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 CFR Part 2 and other Federal regulations. The California Health & Safety Code (HSC) Section 1280.15 (Health Facilities Data Breach), California Medical Information Act (CMIA), County Mental Health Pan Agreement, Substance use Disorder Agreements and other State regulations require DPH to investigate, report and notify patients of a suspected breach of patient medical and/or personal information.

B. **Scope:** It is the responsibility of all DPH employees, UCSF employees, affiliates, and contractors to immediately (collectively referred to as "workforce members") report an incident that they become aware of or suspect is a privacy breach to their site Privacy Officer or contact the Privacy and Compliance Hotline. This policy pertains to all individuals at DPH who have access to, use, or disclose PHI or PII regardless of DPH division or department.

II. Definitions:

A. Breach: The acquisition, access, use, or disclosure of protected health information in a manner not permitted by HIPAA which compromises the security or privacy of the protected health information.

(45 CFR 164.402)

B. Business Associate: A person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involves the use or disclosure of individually identifiable health information**.**

C. Licensed Facility: A clinic, health facility, home health agency, or hospice licensed pursuant to sections 1204, 1250, 1725, or 1745 of the California HSC. For the purposes of this policy, the unauthorized access notification requirements of HSC Sec. 1280.15 only apply to Licensed Facilities. [HSC Sec. 1280.15, as amended by SB 541.]

D. Medical Information: Any individually identifiable information, in electronic or physical form, that is in the possession of, or derived from, a provider of health care, health care service plan, pharmaceutical company or contractor, regarding a patient's medical history, mental or physical condition, or medical treatment, or diagnosis. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual. [CMIA, California Civil Code 56.05.]

E. Patient: The term patients include patients, clients and residents.

F. Personally Identifiable Information (PII): An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted (meaning rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security): Social Security Number; Driver license number or CA identification card number; Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; Medical information (any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional); Health insurance information (an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records); or User name or email address, in combination with a password or security question and answer that would permit access to an online account. [California Civil Code §1798.29.]

G. Protected Health Information (PHI): Health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 CFR § 160.103.

H. Secured Protected Health Information: Any PHI which is unusable, unreadable, or indecipherable to unauthorized persons using technology or methodology, such as encryption or destruction, as

specified by the Health and Human Services (HHS) Secretary.

I. Unauthorized Access: Unauthorized viewing of PHI for non-business reasons (reasons unrelated to treatment, payment or operations).

III. Privacy Incident Investigation:

A. **Reporting Requirement:** Workforce members must report any potential privacy breach as soon as possible even if they are not sure a breach has occurred and/or do not have all the information. It is important to report incidents promptly as there are time restrictions and financial penalties regarding reporting to regulatory authorities and notifying patients.

1. Contacts for Reporting:

a. DPH Compliance and Privacy Hotline Telephone: 855-729-6040.

b. DPH Compliance and Privacy Hotline Email: compliance.privacy@sfdph.org.

B. **Investigation:** The DPH site's Privacy Officer will conduct and be responsible for the investigation and risk assessment to determine the probability that PHI or PII have been compromised. OCPA will be responsible for all required notifications.

1. Workforce members involved in the potential breach should not directly contact the patient unless directed to do so by OCPA.

C. **Breach Determination:**

1. **Risk Assessment:** The DPH site Privacy Officer will conduct a HIPAA breach reporting risk assessment based on the facts obtained through the investigation and make the determination if a reportable breach has occurred.

2. **Documentation:** The privacy incident will be filed and logged in the OCPA investigations log. All corresponding documents will be filed in the OCPA investigation case file. OCPA is responsible for maintaining all documentation related to privacy breaches for seven (7) years from the date of the breaches or potential breaches. This documentation will include all notifications associated with the breaches. Documentation will be maintained electronically on the DPH network.

D. **Reporting and Patient Notification:**

1. **Patient Notification:** OCPA will notify DPH patients whose PHI/PII has been breached or improperly disclosed. Notification letters are to be sent out as soon as possible but no later than 60 days from notification of the breach. For ZSFG and LHH patients, patient notification will be carried out by the site's Privacy Officer within 15 days from notification of the breach.

2. **Law Enforcement Delay of Notification:** OCPA shall immediately notify the City Attorney's Office (CAT) for guidance, if a law enforcement official states that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, Upon the direction of the CAT, requests to delay notification will be handled as follows:

    a. If the statement is in writing and specifies the time for which a delay is required, OCPA will delay such notification, notice, or posting for the time specified by the official; or

    b. If the statement is made orally, OCPA will document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in this section is submitted during that time.

    c. In either case, documentation related to the law enforcement delay request will be retained.

3. **Reporting:** OCPA staff is responsible for reporting the breach to regulatory agencies. For ZSFG and LHH reportable breaches, OCPA will notify the appropriate regulatory division to coordinate reporting to CDPH.

    a. **If the breach involves 500 or more individuals**: Notify the Secretary of HHS without unreasonable delay and in no case later than 60 days, (OCR website), the State Attorney General without unreasonable delay (electronic breach only), and the media. OCPA will notify the Chief Communications Officer/Public Information Officer to notify prominent local media outlets about the breach.

    b. If the breach involves less than 500 individuals: Notify the Secretary of HHS (OCR website) by March 1 for those breaches occurring in the prior calendar year. ZSFG and LHH reportable breaches shall be reported to CDPH within 15 business days from the date of the breach notification.

E. **Remediation and Corrective Action:** OCPA is responsible for providing oversight and advisory assistance to the affected division or CBO and to ensure that appropriate remediation occurs. This includes actions such as implementation and ongoing monitoring of process change, technical measures, or individual disciplinary measures designed to prevent a breach in the future. If necessary, even in cases where it has been determined a breach has not occurred, a corrective action plan may be instituted to mitigate potential breaches.

F. **Sanctions and Discipline:** OCPA will refer investigations to determine a workforce member is culpable for the breach to DPH Labor relations for appropriate discipline.

G. **Retaliation Prohibited:** Workforce members may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual reporting a potential privacy breach or who opposes any act or practice that is unlawful under federal 45 CFR Section §164.530(e).

Last Reviewed/Revised Date: 9/10/2009; 4/26/2019; 10/18/2021; 9/11/2023; 2/19/2026