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: B.1.1 REPORTING OF UNLAWFUL OR UNAUTHORIZED ACCESS OF PROTECTED HEALTH INFORMATION/PERSONAL INFORMATION (PHI/PI BREACH REPORTING POLICY)	
Category: Privacy	
Effective Date: 9/10/2009	**Last Reviewed/Revised Date:** 9/11/2023
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:**

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 Personal Information (PI). This policy specifically provides guidance to Office of Compliance and Privacy Affairs (OCPA) staff, DPH employees, affiliates, contracted Community Based Organizations (CBOs), Business Associates and other contracted organizations. 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.

POLICY

It is the policy of DPH to protect patients' personal and medical information. It is the responsibility of all DPH employees, UCSF affiliates and contractors to immediately 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 Protected Health Information or Personal Information regardless of DPH division or department. Additionally, UCSF affiliates and DPH contractors must follow these procedures for incidents involving DPH patients, clients or residents including notifying DPH when breaches are suspected. The term patients will include clients and residents. DPH employees, UCSF affiliates and contractors 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).

Once notified of a potential breach, the Office of Compliance and Privacy Affairs will begin an investigation and risk assessment to determine the probability that the PHI or PI has been compromised. OCPA will be responsible for all notifications to regulatory agencies; Medi-Cal managed care plans and patients. The Office of Compliance and Privacy Affairs (under the direction of the Chief Integrity Officer/Director, Office of Compliance and Privacy Affairs) is responsible for adherence to this policy.

DEFINITIONS

- **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)
- **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 involve the use or disclosure of individually identifiable health information.
- **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]
- **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]
- **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.
- **Personal Information (PI)**
  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

- **Secured Protected Health Information**
  Any PHI which is unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology, such as encryption or destruction, as specified by the Health and Human Services (HHS) Secretary.
- **Unauthorized Access**
  Unauthorized viewing of PHI for non-business reasons (reasons unrelated to treatment, payment or operations).

PROCEDURE

I. Breach Notification

a. **DPH, UCSF and CBO staff should 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 of 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.

b. The site's DPH Privacy Officer will begin an investigation and risk assessment to determine the probability that PHI or PI has been compromised. OCPA will be responsible for all required notifications. For breaches involving social security administration (SSA) data, notification and investigation are to start by one hour after discovery. For breaches involving substance use disorder (SUD)/ODS clients, mental health plan clients and Medi-Cal managed care members, notification to the appropriate regulatory agency or Medi-Cal managed care plan should commence within 24 hours after learning of the potential breach.

c. **The DPH, UCSF or CBO staff involved in the potential breach should not directly contact the patient unless directed to do so by OCPA.**

Contacts for Reporting Breaches

DPH Privacy Hotline (Available to DPH, UCSF and CBO employees)

(855) 729-6040

Email: compliance.privacy@sfdph.org

II. Breach Determination

a. OCPA staff will contact the person reporting the breach and will fill out the incident details on the OCPA Intake Form (Attachment A).

b. OCPA staff in consultation with the Director of OCPA/Chief Integrity Officer will conduct a risk assessment and make the determination if a breach has occurred. (See Attachment C for the factors in determining whether a breach has occurred.)

c. **Once OCPA determines whether a breach has occurred,** the decision-making process and case investigation will be documented on the OCPA Privacy Breach Checklist (Attachment B). The case will be filed (in the OCPA electronic files). The incident or breach will be logged in the Privacy Breaches Case Log.

III. **Notification Process**

a. **Notification Responsibility:** OCPA will notify DPH patients whose PHI/PI 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. (See Attachment C for the notification letter template.)

b. **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:

i. 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 period specified by the official; or

ii. 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 III.b.i. of this section is submitted during that time.

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

IV. Reporting

a. OCPA staff is responsible for reporting the breach to regulatory agencies.

b. 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.

c. 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.

V. Remediation and Corrective Action

a. The Office of Compliance and Privacy Affairs is responsible for providing oversight and advisory assistance to the affected department 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.

VI. Sanctions

a. If warranted, OCPA in consultation with Human Resources will recommend sanctions. If the breach was caused by unauthorized access, it can result in the DPH employee's termination of employment.

VII. Documentation

a. 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.

VIII. Administrative Requirements (§164.530)

See policy A2.0 Administrative Requirements that is incorporated in this policy.

REFERENCES

A. Health Insurance and Portability Act (HIPAA) [Title 45 Code of Federal Regulations Part 160, 162 and 164.
B. Health Information and Technology for Economic and Clinical Health (HITECH) Act
C. Breach Notification Rule (OCR Guidance)
D. California Civil Code §56.05 (California Medical Information Act-CMIA)
E. California Civil Code §1798.29 (California Breach Notification Requirements)
F. California Health & Safety Code section 1280.15 (Health Facilities Data Breach)

ATTACHMENTS

A. OCPA Intake Form
B. OCPA Privacy Breach Checklist
C. Privacy Breach Risk Assessment
D. Breach Notification Letter Process and Template

ATTACHMENT A

OCPA Intake Form

Case #	
Date:	
Investigation Officer:	

Communicated By:	
Last Name:	**Department:**
First Name:	**Phone:**
Is the caller a: ☐ Staff ☐Faculty ☐Patient ☐Volunteer ☐Contractor ☐ Other:	
On behalf of:	
Name:	MRN#
Intake Information:	
Resolution:	
Resolution Date:	
Outcome of Case:	
Patient Notification Date:	
CDPH or DHCS Notification Date:	

ATTACHMENT B

Privacy Breach CHECKLIST

(**To be completed by Office of Compliance and Privacy Affairs)**

ACTION BY OCPA:	DATE	NOTES
1. Receive Notification of potential breach		
2. For MH plan, SUD or ODS services, notify DHCS within one hour if SSA file information involved. If potential breach involves a SFHP Medi-Cal managed care member, MH plan services or SUD/ODS services, notify SFHP or DHCS within 24 hours.		
3. Log incident & Interview reporter and/or Supervisor		Log incident and create a file
4. Determine if incident is a privacy breach		Conduct risk analysis per step #5 Privacy Officer/Investigations Officer consults with Chief Integrity Officer/Director, OCPA regarding whether the incident is a reportable breach. Consult with CAT as needed.
5. Breach Risk Analysis:	Y/N	See Attachment C
1. Unintentional acquisition-workforce member		45 CFR 164.402(1)(i)
2. Inadvertent disclosure-workforce member		45 CFR 164.402(1)(ii)
3. Unauthorized person unlikely to retain		45 CFR 164.402(1)(iii)
If no to above questions, then evaluate		
i) The nature and extent of the PHI involved		
ii) Unauthorized person		
iii) Whether PHI accessed/viewed		
iv) Extent PHI risk mitigated		
- Was electronic device involved encrypted?		If so, safe harbor and no breach has occurred
- Determine if incident meets California PI breach criteria		
6. Notify relevant Privacy Officer (if CBO) of breach decision		

ACTION BY OCPA:	DATE	NOTES
7. If not a reportable breach, determine if corrective action is needed		If warranted, OCPA sends corrective action plan to Supervisor. Go to Step #28
8. If incident involves a lost or stolen electronic device (laptop, cell phone USB, etic), notify IT Security		Confirm that DPH IT Help Desk/Security has been notified. Confirm that the device has been wiped clean.
9. If a ransomware attack, IT Security must notify the FBI field office		Also, IT to report incident to the FBI's Internet Crime Complaint Center (www.ic3.gov).
10. If the breach involves unauthorized access		Notify the Service Desk to disable access to all systems. If DPH employee, notify Labor to remove employee from areas where PHI is handled. If UCSF employee, coordinate with the Dean's Office.
11. If law enforcement requests delay in notification or reporting, notify City Attorney Office		If law enforcement requests (verbally or in writing) for DPH to delay notification/reporting OCPA notifies the City Attorney for guidance.
12. Request list of affected individuals		Need name, address, primary language, age if minor If a minor, obtain parent or legal guardian name Obtain next of kin if deceased
13. Notify city risk management and City Chief Information Security Officer (CISO) (if electronic data only)		Notify if >500 people or breach is deemed to be significant.
14. If a major breach (>500 people), implement emergency response procedure		
15. Notify OCR if ≥500. Notify the State Attorney general (if >500 people and electronic data only)		**Notify OCR immediately if breach is over 500 individuals.** Notify CA Attorney General without unreasonable delay (breach of electronic data only): https://oag.ca.gov/ecrime/databreach/report-a-breach 1. Attach sample patient notification letter 2. Fill out form and submit Checks state AG database (right side of form page) to confirm receipt of letter and form. Case number will be in URL

ACTION BY OCPA:	DATE	NOTES
16. Notify the media (if >500 people affected)		Contact Chief Communications Officer/Public information Officer (PIO) to coordinate notifying the media PIO to post notice on www.sfdph.org website
17. Substitute breach notification (if cost of notification exceeds $250,000 or affected individuals is over 500,000). For HIPAA breaches, this substitute breach notification does not apply		Elements of Substitute Breach Notice: 1. Email notice to those with addresses 2. Conspicuous posting for a minimum of 30 days on DPH public web page 3. Notify statewide media and Information Security Office http://www.cio.ca.gov/OIS/ Per CSIO email 11/24/15-Notify the California Information Security Office (CISO) by email at security@state.ca.gov. Within the email, provide a description of the security incident, the root cause of the security incident (if known) and the qualifying factors for utilizing the Substitute Breach Notice provisions.
18. If the potential breach is associated with research, notify the Research Integrity Officer. Researcher to notify the IRB.		OCPA to review IRB decision.
19. If PI is breached, notify DHCS: a Submit DHCS PRIVACY INCIDENT REPORT (PIR)		
20. Determine if potential breach involves a San Francisco Health Plan (SFHP) Medi-Cal member and of the services are covered through SFHP.		Determine if patient is a SFHP member and if services are covered. IF YES, go to #21 IF NO, go to step #22
21. If Medi-Cal managed care service and patient was a member at the time of the potential breach: a. Notify SFHP b. Submit draft patient notification letter to SFHP who will submit letter and PIR to DHCS.		Notify SFHP Officer, Compliance & Regulatory Affairs
22. IF PHI was created by a behavioral health provider, determine if the services are covered under the mental health plan, if so, DHCS must be notified:		Determine if service is provided under the Mental Health plan or SUD program contracted through the state.

ACTION BY OCPA:	DATE	NOTES
a Notify DHCS of a privacy incident within 24 hours (one hour if SSA data) b Notify DHCS via secure emailing a DHCS PRIVACY INCIDENT REPORT c If breach involves more than 500 individuals follow major breach steps (starting with step #13) Update PIR within 72 hours. d If DHCS determines it's a breach, submit patient notification letter for approval e Mail approved patient notification letter f Submit a final report with corrective action plan within ten (10) working days of the initial report. If more time is needed, request an extension.		IF YES, continue with step #22 or #23 IF NO, go to step #25 Send completed PIR via SECURE email to PrivacyOfficer@dhcs.ca.gov
23. If substance use disorder service provided under SUD contract with the state, a. Notify DHCS of a privacy incident within 24 hours (one hour if SSA data) b. Notify DHCS via secure emailing a DHCS PRIVACY INCIDENT REPORT c. If breach involves more than 500 individuals follow major breach steps (starting with step #13) d. Update PIR within 72 hours. e. If DHCS determines it's a breach, submit patient notification letter for approval f. Mail approved patient notification letter g. Submit a final report with corrective action plan within ten (10) working days of the initial report. If more time is needed, request an extension. h. If OCR contacts DPH regarding a privacy breach involving client(s) covered by Substance Use Disorder Prevention and Treatment Block Grant (SABG), inform DHCS.		
24. If SUD information is breached in violation of 42 CFR Part 2, then notify the San Francisco office of the US Attorney General. For breaches involving clients in an opioid treatment program (OTP), notify SAMHSA's Division of Pharmacologic Therapies.		

ACTION BY OCPA:	DATE	NOTES
25. Notify the OCR		File online reports for the calendar year to the OCR [60 days end of year] for all breaches affecting fewer than 500 individuals.
26. Notify California DPH (for licensed facility or home health care agency only)		Notification must be done within fifteen (15) business days. Affects ZSFG, LHH, and Home Health. OCPA will work with Regulatory Affairs at the facility coordinate this notification.
27. Notify licensing board (if applicable)		Notify applicable licensing board if the person committing the breach is a licensed professional
28. Notify patients. Per HIPAA & state regulations, include (1) what happened, the date of breach and the date of discovery, (2) a description of the types of unsecured PHI (3) steps patients should take to protect themselves from economic or other harm, (4) what is being done to investigate the breach and mitigate harm, and (5) contact procedures. Must state **"SUBJECT: NOTICE OF DATA BREACH"**		If Mental Health plan member or SUD or ODS client, this letter must first be approved by DHCS before OCPA issues letter. If SF Health Plan member, DPH letter is submitted through SFHP for DHCS approval. Coordinate with CCSF Reprographic for high volume notices.
28. Send Corrective Action Plan (CAP). CAP should be sent as needed for a privacy incident.		Establish implementation dates
29. Confirm that corrective action has been implemented		
30. Close file		Complete logging case
31. Log all documents regarding the case in the OCPA electronic case file. Include corrective action responses from regulatory bodies involved in the investigation.		Log communication including fines. **State**- Implement corrective action plan and follow-up with the state **Federal**- Implement (as applicable) voluntary compliance, corrective action or resolution agreement. Follow-up with OCR or federal agency imposing the corrective action.

ATTACHMENT C

Privacy Breach Risk Assessment

OCPA will consider the following when deciding whether a breach has occurred (per Federal code §164.402).

I. The term "breach" does **NOT** include:

- **a.** Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA) if the acquisition, access or use was made in good faith and within the course and scope of the authority and does not result in further use or disclosure in a manner not permitted by the Privacy Rule.
- **b.** Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement (OHCA) in which the CE participates, and the information received is not further used or disclosed in a manner not permitted by the Privacy Rule.
- **c.** A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
- **d.** Devices that are lost or stolen that contain PHI if the devices are encrypted (and meet DPH standards).

II. If the incident does not meet the criteria in II.b.i.1, then OCPA will determine if a breach has occurred based on a risk assessment of at least the following factors:

- **v)** The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
- **vi)** The unauthorized person who used the PHI or to whom the disclosure was made
- **vii)** Whether the PHI was acquired or viewed
- **viii)** The extent to which the risk to the PHI has been mitigated

III. **Safe Harbor** - If PHI is encrypted (rendered unusable, unreadable, or indecipherable to unauthorized individuals) as specified in the HIPAA Security rule and/or follows the National Institute of Standards and Technology (NIST) standards for data at rest and data in motion then there is no reporting requirement, even if a breach occurs.

IV. **Determining a Ransomware Breach:** The OCR has issued guidance regarding determining whether a breach has occurred in a ransomware situation. The guidance can be found here. OCPA in consultation with IT and the CAO as needed, will determine if a breach has occurred due to ransomware. If this is the case, IT will contact the FBI and OCPA will initiate the breach notification process.

ATTACHMENT D

BREACH NOTIFICATION LETTER PROCESS AND TEMPLATE

The breach notification letter process is conducted by OCPA.

California Civil Code 1798. 29 and 45 CFR 164.404 Summary

- Text in the notice must be no smaller than 10-point type
- Notice must be written in plain language. May use specific form in the code or if the form is not used, must use the headings in the form (see page 15-16).
- DPH will send this written notice by first-class mail. If DPH has insufficient or out-of-date contact information for 10 or more individuals, DPH must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside.
- If DPH has insufficient or out-of-date contact information for fewer than 10 individuals, DPH will provide substitute notice by an alternative form of written notice, by telephone, or other means.
- If DPH knows that the individual is deceased and has the address of the next of kin or personal representative of the patient, written notification to that contact person shall be sent.
- For a breach (involving electronic data) of 500 individuals or over, an electronic submission of a single copy of the security breach notification must be sent to the state Attorney General. The on-line form to comply with this provision is here: https://oag.ca.gov/ecrime/databreach/report-a-breach

State and HIPAA Breach Notification Letter Format

Required Elements:

Subject: NOTICE OF DATA BREACH

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* and was discovered on [*date of discovery of incident]* at *[name of organization*]. An employee inadvertently e-mailed a document containing your personal information to the wrong person.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*][1] Please note, the information was limited to [*specify, (e.g., your name and medical treatment)*] and did not contain any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft. Nonetheless, we felt it necessary to inform you since your medical information [*or medical history, medical condition, or medical treatment or diagnosis*] was involved.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your [provider or plan], to serve as a baseline.

Other Important Information:	Enclosure "Breach Help –Consumer Tips from the California Attorney General" **Propose:** Enclosure: Placing a Free Fraud Alert on Your Credit Files {when potential identity theft is possible such as disclosure of social security numbers}
Law Enforcement Delay	Note if the delay of notification was authorized for law enforcement purposes
For More Information:	For information about your medical privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection at www.privacy.ca.gov.
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*phone number*].

Last Revision Date: 4/26/2019

10/18/2021

9/11/2023

Last Reviewed Date: 9/11/2023