



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: Use of Protected Health Information in Disciplinary Investigations and Proceedings	
Category: Privacy	
Effective Date: TBD	Last Reissue/Revision Date: November 16, 2022
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 <input checked="" type="checkbox"/>	If not DPH-wide, other distribution:

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

1. POLICY

It is the policy of the San Francisco Department of Public Health (DPH) to have a process in place for providing de-identified patient protected health information (PHI) to employee representatives who have requested such information pursuant to a disciplinary matter.

2. PURPOSE

To comply with Federal and State privacy laws and to ensure that employee representatives properly access confidential information that is material to a disciplinary action while maintaining patient, client, and resident rights to the privacy of their PHI.

Pursuant to the due process protections outlined in Skelly vs. State Personnel Board, DPH recognizes the right of employee representatives to have access to all materials supporting a proposed disciplinary action. ZSFG Administrative Policy 8.21 applies to the access and use of PHI that is not contained in the documents that are provided to an employee as part of the Skelly process.

3. PROCEDURE

- A. An employee representative who seeks access to PHI for purposes of representation in a disciplinary matter shall submit a written request to the DPH Human Resources Labor Division.

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. Requests for information will be processed, unless the requests involve a large volume of documents, or the DPH Human Resources Labor Division is concerned that the request is overly broad or vague. In those cases, a time shall be arranged for the employee representative to go to the appropriate Medical Records Department within DPH to review the records. The employee representative shall then mark the documents that he or she wishes to have copied. If a dispute remains regarding the request, the parties shall meet and confer. The parties will make reasonable adjustments to disciplinary and grievance timelines during the pendency of any such dispute. If the parties cannot reach an agreement within 30 days of the date originally scheduled for the Skelly meeting, the Department will proceed with the disciplinary process.
- C. Absent a dispute over the scope, or once agreement has been reached, the Medical Records Department shall copy the requested records, redact patient identifying information, and forward the records to the DPH Human Resources Labor Division.
- D. The DPH Human Resources Labor Division shall forward the records to the employee representative.
- E. Upon conclusion of the disciplinary matter, the employee representative shall return the records to the DPH Human Resources Labor Division, which, in turn, shall return the records to the Medical Record Department for filing or destroying.
- F. If either an employee or human resources representative wishes to speak directly with a patient or client, that request shall be submitted from the DPH Human Resources Labor Division to the appropriate DPH Risk Management Division. DPH Risk Management shall contact the patient's/client's primary provider, or upon request, another member of the care who is responsible for the patient. The primary provider shall then contact the patient /client and ask whether s/he is willing to speak with the employee and human resources representatives and, if yes, to arrange for a time for a joint interview.
- G. An employee representative may not access PHI directly (i.e. viewing medical records, whether it be paper documents or electronic records, or interviewing patients/clients). Such an act may result in disciplinary action against the employee representative (if that employee representative is also a DPH employee), or barring that employee representative from DPH facilities.

4. REFERENCES

DPH Policies:

[DPH Policy A.1.0 – Privacy Policy](#)

[DPH Policy A.2.0 – HIPAA Compliance – Admin Policies](#)

[DPH Policy A.3.0 – HIPAA Compliance – Patient/Client/Resident Rights regarding Protected Health Information \(PHI\)](#)

[DPH Policy B.1.1 – Reporting of Unlawful or Unauthorized Access of PHI \(Potential Breach\)](#)

[DPH Policy B.2.0 – Major Privacy Breach Emergency Quick Reference Response Guide](#)

[DPH Policy C.1.0 - Authorization for Use and Disclosure of PHI](#)

[DPH Policy D.1.0 – Secure Delivery of PHI Policy](#)

[DPH Policy D.1.1 – FORM: Secure Delivery of PHI – Cover sheet for fax or mailing](#)

[DPH Policy D.1.2 – Sending Electronic Messages to Adult Patients](#)

[DPH Policy E.1.0 – Privacy and the Conduct of Research](#)

DPH-Wide Administrative Policy 9.09 – Request for DPH/SFHN Epic Network Access

ZSFG Administrative Policies:

8.05 HIPAA Compliance: Privacy Policy

8.10 HIPAA Compliance: Administrative Requirements

8.11 HIPAA Compliance: Authorization for Use and Disclosure of Protected Health Information

8.12 HIPAA Compliance: Privacy and the Conduct of Research

8.13 HIPAA Compliance: Patient/Client/Resident Rights Regarding Protected Health Information

8.14 HIPAA Compliance: Policy for Secure Transmission of protected Health Information (PHI)

8.15 HIPAA Compliance: Security Policy Violation - Discipline and Sanctions

8.19 HIPAA Compliance: Contingency and Business Continuity Planning Policy

8.20 HIPAA Compliance: Policy for Classification of Information

8.23 HIPAA Compliance: Policy for Secure Disposal or Reuse of Media Containing Critical Data

8.24 HIPAA Compliance: Wireless Network and Information Transmission Security Policy

8.25 HIPAA Compliance: Security Documentation and Accountability Policy

8.26 HIPAA Compliance: Security Activity Logging, Tracking and Reporting Policy

8.27 – Breach Notification Policy

9.09 Information Systems: Request for Community Health Network Access