San Francisco Department of Public Health

*Policy & Procedure Detail**

Policy & Procedure Title: C.12.0 Social Media Policy	
Category: Privacy	
Effective Date: 7/6/2015	**Last Reissue/Revision Date:** 3/16/2026
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 X	**If not DPH-wide, other distribution:**

All sections in table required.

I. **Purpose and Scope:**

A. **Purpose:** The Social Media policy is designed to provide guidance to San Francisco Department of Public Health (DPH) and University of California San Francisco (UCSF) affiliated staff regarding use of social media, including that which is DPH-sponsored as well as the personal use of social media as it pertains to DPH work-related responsibilities and representations of the department. It is the intent of this policy to support the effective and responsible use of social media, protect the privacy of DPH clients and staff, and to ensure compliance with Federal HIPAA and State privacy and security regulations.

B. **Scope:** This policy applies to all DPH workforce members, including employees, affiliated staff and residents, contracted staff, students, volunteers, medical staff, and individuals representing or working at DPH. This policy applies to the use of DPH-sponsored or approved social media, as well as the use of personal and non-DPH-sponsored social media.

II. **Definitions:**

A. **Protected Health Information (PHI):** Any medical identifiable information (verbal, written, or electronic) about a patient, resident, or client's physical or mental health, the receipt of health care, or payment for that care.

B. **Patient Identifiable Information (PII):** Any individually identifiable information regarding an individual, including their name, address, date of birth, Social Security Number, account number, security code, driver's license number, financial or credit account numbers, phone numbers, Internet domain addresses, social media handles, and other personal identifiers.

C. **Social Media:** Social media includes websites and applications that allow users to create and share content or to participate in social networking. These websites and applications may

include, but is not limited to, blogs, social networks, bookmarking sites, social news, media sharing, microblogging, blog comments and forums, social review sites, or other websites or discussion forums.

III. **Personal Use of Social Media:**

A. **Prohibition:** DPH employees shall never disclose client, patient, or resident PHI, PII, or any other information through social media of any kind without the express written permission obtained through DPH or a facility administration's approval process. Use of personal social media accounts and networks, including social media applications on personal electronic devices, should not occur during work hours, and in strict compliance with all other DPH and facility-specific policies regarding use of organizational assets or City resources.

1. This includes posting PHI or PII, information, screenshots, or sharing links to photos, images, video, recordings, text, or other information that could reasonably lead to the identification of a client, patient, DPH staff, or resident.

B. **Written Authorization Required:** Do not post or share photos, videos, PHI or PII, or other information about clients, patients, DPH staff, or residents without their written consent.

C. **Violation of Law and Policy:** Disclosure of any such information about a client, patient, DPH staff, or resident is a violation of the Health Insurance Portability and Accountability Act (HIPAA), other federal privacy or security laws, California's Confidentiality of Medical Information Act (CMIA), other state privacy laws, and/or DPH or DPH facility-specific policy.

D. **Examples of Prohibited Conduct:** Examples of conduct that may violate federal and state privacy laws, as well as this and other CCSF/DPH policies include but are not limited to:

1. Any photo or video taken within a DPH facility or clinic of a client/patient/resident, or health information of a client/patient/resident, without written authorization.

2. A photo of a workplace lunch may violate HIPAA and other privacy rules if there is any visible patient information in the photo, including in the background.

3. Posting verbal "gossip" about a patient to unauthorized individuals, even if the name is not disclosed.

4. Sending a tweet about a patient who is routinely late to appointments.

5. Posting a photo of a patient's x-ray (even without the patient's name) to Instagram.

6. Reposting a photo of an empty but used trauma room that had been used to treat an individual who had been in a car accident with the caption "#womanvscar."

7. Soliciting health-related information, such as asking what type of medication someone is taking.

8. Sharing of photos, videos, or texts on social media platforms within a private group.

E. **Messaging:** Private or direct messages on social channels or texting applications are not HIPAA or CMIA approved for communicating with patients about private health-related information.

1. Do not participate in social media discussions with patients who have shared PHI on social media.

2. Examples of social channels that are not approved include, but are not limited to, Facebook Live, Twitch, TikTok, Slack, and other texting applications.

3. Do not disclose private information of other DPH staff, or refer to other DPH staff in a harassing manner.

4. Staff members should consult with their supervisor if they are unsure whether any DPH related or client/patient/resident information is confidential, but should refrain from posting anything online or sharing any information.

IV. **Best Practices:**

A. **If unsure, do not post anything.** If you do not have the written consent to share information about a client, patient or resident, even if it does not mention the patient's name, then **DO NOT POST IT**.

B. **Keep Personal Use Separate from Work.** You may not use a DPH-issued email address for personal use of social networking sites. Personal social media accounts may not use "DPH" or any acronyms for it or any DPH facility or clinic in the name and may not use the DPH or any DPH facility or clinic logo or branding.

C. **Be Transparent.** If you identify yourself as DPH faculty or staff in any online social medium or network, or your affiliation with DPH could be presumed, you must make it clear that you are not speaking on behalf of DPH. Use this statement: ***"The views expressed here are my own and not on behalf of my employer, SF DPH."***

D. **The Internet is public.** Remember that any social media post or comment, whether public or private, may be viewed by leadership, patients, prospective patients, and the media.

E. **Know and follow CCSF and DPH facility-specific social media policies.**

F. **Report any potential HIPAA violations.** Call the DPH Compliance and Privacy Hotline at 1-855-729-6040 and/or email compliance.privacy@sfdph.org and notify that office of any potential HIPPA violation.

V. **DPH-Sponsored Use of Social Media:**

A. **Work-Related Purpose:** DPH sponsored or work-related social media accounts may be appropriate tools for achieving organizational objectives, however must be coordinated with and authorized through Division Directors and the Director of Communications.

B. **Consent Required**: DPH staff shall not post or share photos, videos, or other information about clients, patients, or residents without their written consent.

1. If a communication plan for DPH sponsored use of social media would include posting photos or videos, or patient information in any format, including written, then staff

must obtain appropriate written authorization and consent forms from all persons in the photos or videos, including clients, patients, or residents. Consent may also be required for employees, staff, or visitors.

2. Consent forms must be maintained in the department or the patient's medical record for six years after the last day the site is active.

C. **Administrative Approval:** Content and creation on DPH-sponsored social media sites/platforms shall be subject to administrative approval and staff may be required to discontinue use if deemed inappropriate by Administration. Staff must create and get approval through their division director for a communication plan when DPH staff members are initiating conversations or alerts to the public using social networking sites. Communication plans should include the following elements:

1. Objectives;

2. Plan for responding to comments;

3. Plan for frequency of review for inappropriate content; and

4. Consultation with the City Attorney's Office, as necessary.

D. **Legal Requirements:** DPH authorized accounts must follow all copyright laws.

E. **Employee Responsibility:** DPH employees are expected to adhere to DPH rules of conduct and regulations when using or participating in DPH sponsored social media including protecting privacy of patient health information, privacy of other DPH employees and affiliates and confidential hospital information.

F. **Disclaimer:** Administrators of DPH sponsored interactive social media (such as Facebook) shall include a disclaimer statement ***"The views expressed in this forum do not necessarily reflect those of the San Francisco Department of Public Health. We reserve the right to remove any posts or comments that violate patient confidentiality, are offensive, inappropriate or excessive."***

1. Threatening or obscene comments may be deleted, as well as spam, posts promoting illegal activities, or copyright infringements.

2. Selling advertisements by departments on DPH-sponsored social media is prohibited.

VI. **Violations and Enforcement:**

A. **Ceasing of Activities:** DPH reserves the right to request to have online communications stop if DPH believes communications from an employee, physician, fellow, resident, volunteer, and/or students are in violation of organizational policies; CCSF/DPH policies or values; or state and/or federal privacy laws.

B. **Sanctions:** Violations of this Policy will be reported to the appropriate department. Violations will be investigated to determine the nature, extent and potential risk to the hospital and/or DPH. Violations under the HIPAA Privacy Rule may incur penalties (which can result in fines of $100,000-$1,500,000 to the organization or individual), and/or criminal penalties (which may

result in fines from $50,000 to $250,000 and up to 10 years in prison. Violations of California privacy laws may include the following penalties:

1. For the individual: fines up to $25,000 per violation ($250,000 maximum), possible misdemeanor charge if economic loss or personal injury, potential for civil action, Cal-OHI may notify licensing board for further investigation or discipline of individual providers. (California Civil Code 56.36)

2. Institutional fines: $25,000 initial violation per client ($250,000 maximum). (CA Health & Safety § 1280.15)

Last Reviewed Date: 11/1/2021; 9/11/2023; 3/16/2026