I. Policy Statement

The Social Media policy is designed to provide guidance to DPH-SFGH and UCSF affiliated staff regarding use of social media including that which is DPH-SFGH-sponsored as well as the personal use of social media as it pertains to DPH-SFGH work related responsibilities and equipment. It is the intent of this policy to support the effective and responsible use of social media, protect the privacy of DPH-SFGH patients and staff and to ensure compliance with Federal HIPAA and State privacy regulations.

Social media includes items such as blogs, podcasts, websites, discussion forums, and social networks (i.e. Facebook, YouTube, Twitter, LinkedIn). See Appendix A Social Media definitions.

II. Application of Policy

a. This policy applies to all DPH-SFGH workforce members including employees, residents, contracted staff, students, volunteers, medical staff and individuals representing or working at DPH-SFGH.

b. The policy applies to the use of DPH-SFGH sponsored or approved social media, personal and non-DPH-SFGH sponsored social media.

III. Personal Use of Social Media

Use of personal social media accounts, including social media applications on personal electronic devices, should be restricted to incidental use during work time and in strict compliance with all other DPH and SFGH policies regarding use of organizational assets.

a. Protecting Patient Confidentiality

DPH-SFGH employees shall never disclose patient information through social media of any kind without the express written permission obtained through SFGH Administration’s approval process. This includes:

- Protected Health Information (PHI) – Any medical identifiable information (oral, written or electronic) about the patient’s physical or mental health, the receipt of health care, or payment for that care.

- Patient Identifiable Information (PII) – Any individually identifiable information regarding their; name, address, Social Security
Number, account number, security code, driver’s license number, financial or credit account numbers, phone numbers, and Internet domain addresses, and other personal identifiers.

· Posting or hyper-linking to photos, images, video, recordings, text, or other information that could reasonably lead to the identification of a patient.

· Disclosure of any such information is a violation of the Health Insurance Portability and Accountability Act (HIPAA) and/or SFGH policy.

b. You may not use a DPH issued-email address for personal use of social networking sites.

c. Staff members should consult with their supervisor if they are unsure whether any DPH-SFGH related or patient information is confidential.

d. Do not disclose private information of other DPH-SFGH staff, or refer to other DPH-SFGH staff in a defamatory, abusive or harassing manner.

e. Transparency: If you identify yourself as DPH-SFGH’s faculty or staff in any online social medium or network or your affiliation with DPH-SFGH could be presumed, you must make it clear that you are not speaking for DPH-SFGH. Use this statement: “The views expressed here are my own and not those of my employer.”

f. Be aware that any social media conversation, whether public or private, may be subject to public disclosure.

IV. Use of DPH-SFGH Sponsored Social Media

DPH-SFGH related or sponsored social media accounts may be appropriate tools for achieving organizational objectives, however must be coordinated with and authorized through SFGH Administration.

a. Content shall be subject to administrative approval and staff may be required to discontinue use if deemed inappropriate by Administration.

b. DPH-SFGH authorized accounts must follow all copyright laws.

c. Employees are expected to adhere to SFGH and DPH rules of conduct and regulations when using or participating in DPH-SFGH sponsored social media including protecting privacy of patient health information, privacy of other SFGH employees and affiliates and confidential hospital information.
d. Administrators of DPH-SFGH sponsored interactive social media (such as Facebook) shall include a disclaimer statement, “The views expressed in this forum do not necessarily reflect those of San Francisco General Hospital and Trauma Center. We reserve the right to remove any posts or comments that violate patient confidentiality, are offensive, inappropriate, or excessive.”

V. Compliance

DPH-SFGH reserves the right to request to have online communications stop if DPH-SFGH believes communications from an employee, physician, fellow, resident, volunteer, and/or students are in violation of organizational policies, values or local, state or federal laws privacy laws.

a. 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. Employees who violate this policy will be subject to the appropriate disciplinary action up to and including fines for both individual and hospital, loss of licensure or termination.

- California privacy laws include the following possible penalties:

- 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. (AB211- Civil Code 56.36 /Health & Safety § 130200)

- Institutional fines: $25,000 initial violation per patient ($250,000 maximum) (SB541- Health & Safety § 1280.15)

VI. Related Documents

A. DPH Electronic Data Security Policies – User Brief
B. SECURE TRANSMISSION OF PROTECTED HEALTH INFORMATION Policy I.D. 2.0
C. POLICY FOR SECURE STORAGE, DISPOSAL OR REUSE OF MEDIA CONTAINING CRITICAL DATA Policy II.D1.0
D. SECURITY POLICY VIOLATION DISCIPLINE Policy I.A.2.0
E. DPH Social Media Policy

Appendix A.

Definition of Social Media

Social media is the use of electronic and Internet tools for the purpose of sharing and discussing information and experiences with other human beings. When information is shared through the use these tools, conversation and interaction between groups of people is promoted.
The most common examples include the following:

- Blogs (Web logs), i.e. *DiabetesMine, WebMD, YouTube* videoblogging platform
- Instant Messaging (IM), i.e. AOL Instant Messenger- may include web-cams, Skype
- Music-sharing/File sharing
- Podcast, i.e. *John Hopkins Medical Podcasts, CDC Travelers Health, dLife podcasts for diabetes*
- Photo-sharing, i.e. *Flickr*
- Websites
- Social bookmarking, i.e. *Del.icio.us, StumbleUpon, Connotea*
- Social networking, i.e. *Facebook, MySpace, LinkedIn, Twitter, PatientsLikeMe, DailyStrength, ReliefinSite*
- Virtual Worlds
- Whiteboards (frequently used in virtual meeting settings)
- Wikis, i.e. *Wikipedia.org, FluWiki, WiserWiki*

**Source:** AHIMA Advantage" e- Alert (Vol 12, Issue 40)
Dolan, Marsha; Wolter, Julie. "Using Social Media to Promote the Use of a Personal Health Record (PHR) and the Management of Personal Health Information to Consumers." 2009 AHIMA Convention Proceedings, October 2009.

**Cross Reference**

8.05 HIPAA Privacy Policy
8.07 HIPAA Compliance: Retention, Storage and Destruction of Protected Health Information
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
8.16 HIPAA Compliance: Access Control Policy
8.17 HIPAA COMPLIANCE: Portable Computers and Devices Policy
8.18 HIPAA COMPLIANCE: workstation, data display and printout security policy
8.19 HIPAA Compliance: Contingency and Business Continuity Planning Policy
8.20 HIPAA Compliance: Policy for Classification of Information
8.21 USE OF PROTECTED HEALTH INFORMATION IN DISCIPLINARY INVESTIGATIONS AND PROCEEDINGS POLICY

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


8.25 HIPAA Compliance: Security Documentation and Accountability Policy

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

8.27 Reporting Privacy a Breach

APPROVAL
NAF: 9/4/12
MEC: 8/18/12
QC: 8/16/12

Date Adopted: 9/12
Reviewed:
Revised: