The following reflects the findings of the Department of Public Health during a complaint/breach event:

**Complaint Intake Number:**
CA00259998 - Substantiated

Representing the Department of Public Health:
Surveyor ID # 26616, HFEN

The inspection was limited to the specific facility event investigated and does not represent the findings of a full inspection of the facility.

Health and Safety Code Section 1280.15(a) A clinic, health facility, home health agency or hospice licensed pursuant to Section 1204, 1250, 1725, or 1745 shall prevent unlawful or unauthorized access to, and use or disclosure of, patients' medical information, as defined in subdivision (g) of Section 59.05 of the Civil Code and consistent with Section 130203. The department, after investigation, may assess an administrative penalty for a violation of this section of up to twenty-five thousand dollars ($25,000) per patient whose medical information was unlawfully or without authorization accessed, used, or disclosed, and up to seventeen thousand five hundred dollars ($17,500) per subsequent occurrence of unlawful or unauthorized access, use, or disclosure of that patients' medical information.

Violation of Health & Safety Code 1280.15(a) for failure to prevent unauthorized disclosure of patients' medical information Substantiated.

**Action(s):**
- The EMR 1 employee involved in this privacy breach was actually an EMR 2 at the time of this incident and had been oriented to their responsibilities to protect the confidentiality of patient protected health information (PHI) and to medical information privacy at the time of their new resident orientation privacy training (June 19, 2009) and at annual privacy briefing (November 16, 2010) (see Attachment 1, 2)
- April 21, 2011
- The EMR 2 signed a confidentiality statement and had received privacy training by the UCSF Privacy Office as part of his emergency medicine training (see Attachment 3). The EMR 2 was licensed by the Medical Board of California on October 20, 2012.
**Informed Medical Breach**

Health and Safety Code Section 1280.15(b)(2), "A clinic, health facility, agency, or hospice shall also report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information to the affected patient or the patient's representative at the last known address, no later than five business days after the unlawful or unauthorized access, use, or disclosure has been detected by the clinic, health facility, agency, or hospice."

The CDPH verified that the facility informed the affected patient(s) or the patient's representative(s) of the unlawful or unauthorized access, use or disclosure of the patient's medical information.

On 5/18/11, the UCSF Risk Manager at SFGH and the SFGH Director of Risk Management disclosed the incident to the patient's mother.

1280.15(a) Health & Safety Code 1280

(a) A clinic, health facility, home health agency, or hospice licensed pursuant to Section 1204, 1250, 1725, or 1745 shall prevent unlawful or unauthorized access to and use or disclosure of, patients' medical information, as defined in subdivision (g) of Section 56.05 of the Civil Code and consistent with Section 130203. The department, after investigation may assess an administrative penalty for a violation of this section of up to twenty-five thousand dollars.

---

**Upon notification by the Emergency Medicine Residency Director at UCSF, the UCSF Privacy Office instructed the EMR2 to remove the narrative from his Facebook page.**

The SFGH CEO, UCSF Associate Dean, and SFGH Privacy Officer issued a joint memo to all SFGH staff regarding protecting patient confidentiality at SFGH and specifically instructed that with respect to social media, "It is inappropriate to describe a specific clinical case on social media (for example, Facebook, MySpace, Twitter, blogs, etc.) (see Attachment 4).

The UCSF Emergency Medicine Assistant Residency Director met with EMR 2 to discuss the incident and expectations of him.

The UCSF Emergency Medicine Residency Director met with EMR 2 to discuss the incident and expectations of him.

The UCSF Privacy Officer and Director of Risk Management in-serviced the UCSF Emergency Medicine residents on the topic of patient privacy and social media with a focus on not posting any information related to patient care or clinical work online (see Attachment 5).

The SFGH Chief of Emergency Medicine and the UCSF Emergency Medicine Residency

---

**Event ID: KBRT111**

10/22/2012 12:29:44PM

**LABORATORY DIRECTOR'S OR PROVIDER/SUPPLIER REPRESENTATIVE'S SIGNATURE**
Director together met with EMR2 to discuss the incident and expectations of him.

Following the in-service, the Emergency Medicine residents, including EMR2, signed a statement acknowledging that they read and received a copy of the UCSF Department of Emergency Medicine Patient Privacy and Social Media Policy (see Attachment 6).

Before and after this privacy breach incident in 2011, hospital and UCSF leadership have engaged in ongoing efforts via memos, emails, staff trainings, and employee annual update training to ensure that hospital staff are educated and knowledgeable about hospital, UCSF, and SFDPH privacy and security policies.

The SFGH multidisciplinary Privacy Committee, composed of the SFGH Privacy Officer and staff from the SFGH Privacy Office, the SFGH Chief Medical Officer, the SFGH Chief Communications Officer, representatives from the SFGH Legal Affairs, Regulatory Affairs, Health Information Systems departments, as well as representatives from both the SFGH and UCSF Risk Management and Information Systems Departments, meets monthly to review, discuss, and recommend policy involving privacy compliance issues.

In follow-up to a review of facility-related privacy breach cases reported to CDPH conducted by the SFGH Privacy Officer with

<table>
<thead>
<tr>
<th>Event ID: KBRT11</th>
<th>10/22/2012 12:29:44 PM</th>
<th>LABORATORY DIRECTOR'S OR PROVIDER/SUPPLIER REPRESENTATIVE'S SIGNATURE</th>
</tr>
</thead>
</table>

Any deficiency statement ending with an asterisk (*) denotes a deficiency which the institution may be excused from correcting providing it is determined that other safeguards provide sufficient protection to the patients. Except for nursing homes, the findings above are disclosable 90 days following the date of survey whether or not a plan of correction is provided. For nursing homes, the above findings and plans of correction are disclosable 14 days following the date these documents are made available to the facility. If deficiencies are cited, an approved plan of correction is requisite to continued program participation.
Continued From page 3

his Facebook page. He said Patient 1 was involved in a motor vehicle accident and was treated in the emergency department by EMR 1 on 6/1/11. The Director of Regulatory Affairs stated EMR 1 did not use Patient 1's name and medical record number but the Facebook posting included website links related to the accident. UCSF medical residents do clinical rotations at SFCH as part of their training.

In an interview on 6/1/11 at 10:20 a.m., Staff A stated his office was made aware of a possible breach of protected health information (PHI) on 5/9/11, when staff were talking about the postings on the personal Facebook page of EMR 1. He stated the Facebook page was deleted on 5/10/11.

In an interview on 6/1/11 at 10:25 A.M., the UCSF Privacy Officer stated that during the investigation, EMR 1 was asked for his e-mail and the content of what was on his Facebook page. He said that in the narrative posting on Facebook, EMR 1 mentioned privileged information that he would only have known as a doctor involved in the care of Patient 1. He added that the information EMR 1 posted, together with the website links might be enough to identify Patient 1 because of the geographic location of the accident, date of incident and name of the hospital where Patient 1 was treated.

On 6/1/11, the facility provided the website links posted on the Facebook page of EMR 1. On 6/2/11, the website links were searched on the Internet to review and verify the contents of the website links. The four website links indicated the

SFCH managers at the monthly Management Forum meeting, including this 2011 incident, the SFCH Chief of Staff and SFCH Privacy Officer presented the same review to the Chiefs of Service at a Medical Executive Committee (MEC), reminding the chiefs about the hospital and SFDPH privacy and security policies, as well as the penalties for violating these policies and the penalties for violating provisions of SB541 and AB211 (see Attachment 7).

The SFCH Privacy Officer and the SFCH Privacy Analyst routinely conduct "Privacy Rounds" within the hospital departments to educate hospital staff about privacy security and awareness, to validate staff knowledge regarding privacy security and awareness, as well as to identify issues requiring corrective action by managers. Findings are reported to the Privacy Committee (see Attachments 3, 9, 10).

SFCH hospital leadership created new Admin Policy 8.29 Policy for Social Networking and Other Web-Based Communications to provide guidance to staff regarding use of social media as it pertains to work related responsibilities and equipment (see Attachment 11).
Continued from page 4

In-servicing of hospital and UCSF-affiliated staff on the new Admin Policy 8.29 / Policy for Social Networking and Other Web-Based Communications to provide guidance to staff regarding use of social media as it pertains to work related responsibilities and equipment is in progress.

The SFGH CEO issued a memo via email to SFGH and UCSF-affiliated staff regarding new SFGH Admin Policy 8.29 / Policy for Social Networking and Other Web-Based Communications implemented to provide guidance to staff regarding use of social media as it pertains to work related responsibilities and equipment is in progress (see Attachment 12).

The SFGH Privacy Officer has incorporated the new SFGH Admin Policy 8.29 / Policy for Social Networking and Other Web-Based Communications in the new hire orientation session regarding HIPPA and privacy information.

The SFGH Privacy Officer or designee is presenting the new SFGH Admin Policy 8.29 / Policy for Social Networking and Other Web-Based Communications at various forums to ensure staff education and participation.
Continued From page 5

Information only to persons who have the right to receive that information. When using or disclosing confidential information, I will use or disclose only the minimum information necessary.

The facility's HIPAA (Health Insurance Portability and Accountability Act) COMPLIANCE: PRIVACY POLICY indicated:

"VII. Authorization for Use and Disclosure .......
A. DPH (San Francisco Department of Public Health) shall obtain an individual's authorization prior to the use or disclosure of PHI for reasons other than DPH treatment, payment or healthcare operations or for purposes required by law."

The employee's action to disclose the patient's medical information on a networking site where the public had access to it violated Health and Safety Code 1280.15, making the hospital subject to the applicable civil money penalty assessment.

... awareness about the use of social media as it pertains to work related responsibilities and equipment

The new SFGH Admin Policy 8.29 / Policy for Social Networking and Other Web-Based Communications is being added to the employee annual Health Stream training.

Monitoring:
The SFGH Privacy Officer and the CHN Senior Information Systems Manager present an annual report regarding privacy issues to the SFGH Quality Council. In addition, they report any incidents of non-compliance with DPH and SFGH privacy policies which occur during the year at the next scheduled SFGH Quality Council.

Responsible Person(s):
SFGH Privacy Officer
CHN Senior Information Systems Manager

Any deficiency statement ending with an asterisk (*) denotes a deficiency which the institution may be excused from correcting providing it is determined that other safeguards provide sufficient protection to the patients. Except for nursing homes, the findings above are disclosable 90 days following the date of survey whether or not a plan of correction is provided. For nursing homes, the above findings and plans of correction are disclosable 14 days following the date these documents are made available to the facility. If deficiencies are cited, an approved plan of correction is requisite to continued program participation.