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

Complaint Intake Number:
CA00363574 - Substantiated

Representing the Department of Public Health:
Surveyor ID # 27886, 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 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 ($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.

For purposes of the investigation, the department shall consider the clinic's, health facility's,
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 7/26/13, the California Department of Public Health was notified by the hospital that they had received notification that a former employee (EMP 5) had posted pictures containing patient private health information (PHI) on his personal Facebook page. The employee had been fired 4 months prior to the incident. The employee had received HIPAA training at time of employment. These Facebook postings were found 4 months after the employee had been fired.
On 10/8/13 at 2 pm, the Director of Human Resources (DHR) stated that EMP 5 was hired on 7/6/12 to work in the housekeeping department within the Environmental Services Department. The hospital terminated EMP 5's employment on 3/22/13, for faxing an unauthorized memo and pictures to multiple departments containing untrue statements about the environmental services of the hospital.

In a concurrent interview and review of photographs printed from Facebook, with the DHR on 10/18/13 at 2 pm, it was revealed that the hospital was notified by an employee of the hospital that they had discovered postings by EMP 5 on a Facebook site on 7/26/13. There were a total of 21 posted pictures of linen and laundry carts, trash containers, and patient care equipment. The posting on the Facebook page also had comments by each photo that they were taken at the hospital. The postings contained a picture of EMP 5 with his name on each of the posted pages. The DHR stated that during the investigation of this potential breach of PHI it was discovered that 3 photographs of medication administration bags posted, contained the names of three separate patients (Patients 1, 2 and 3) in addition to the name of the medication that each of the patients was receiving. The dates on the used patient medication bags posted were in 12/2012.

On 10/8/12, the hospital's employee agreement, titled, "Confidentiality Policy/HIPPA

<table>
<thead>
<tr>
<th>Action:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Policy ECP707, Social Media, was updated immediately following the site visit. 7/2013</td>
</tr>
<tr>
<td>2. Policy C006, Confidentiality, was updated. 8/2013</td>
</tr>
<tr>
<td>3. Policy PR036, Training Staff, was updated. 8/2013</td>
</tr>
<tr>
<td>4. These policies were sent out to all employees.</td>
</tr>
</tbody>
</table>

Plan for continued compliance:

1. All employees receive HIPAA and social media training upon hire and then annually thereafter.

2. Any employee that causes a HIPAA breach received extra education regarding the policy that was breached. They are also reeducated regarding HIPAA. This is done by the Privacy Officer.

Responsible person:

Director of Performance Improvement, Director of Health Information, Director of Information Systems, Director of Human Resources, Privacy Officer.
Acknowledgement Agreement, signed by EMP 5 on 6/26/2012, read, "Any information concerning patient's illness...is strictly confidential. Under the Health Insurance portability and accountability Act ("HIPPA") there are penalties both civil and criminal for failure to comply with HIPPA requirements."