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

Complaint Intake Number:
CA00410134 - Substantiated

Representing the Department of Public Health:
Surveyor ID # 25730, 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, agency's, or hospice's history of compliance with health and safety code requirements.

<table>
<thead>
<tr>
<th>Event ID: LGN011</th>
<th>3/24/2015 10:02:23AM</th>
</tr>
</thead>
<tbody>
<tr>
<td>LABORATORY DIRECTOR'S OR PROVIDER/SUPPLIER REPRESENTATIVE'S SIGNATURE</td>
<td>Title</td>
</tr>
<tr>
<td>By signing this document, I am acknowledging receipt of the entire citation packet.</td>
<td></td>
</tr>
<tr>
<td>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 patient. 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.</td>
<td></td>
</tr>
</tbody>
</table>
this section and other related state and federal statutes and regulations, the extent to which the facility detected violations and took preventative action to immediately correct and prevent past violations from recurring, and factors outside its control that restricted the facility's ability to comply with this section. The department shall have full discretion to consider all factors when determining the amount of an administrative penalty pursuant to this section.

This RULE: is not met as evidenced by:

Based on interview and record review, the hospital failed to protect the confidentiality of Patient 4's protected health information (PHI) when a staff member, Temp 2, intentionally accessed Patient 4's electronic medical record (EMR) without business justification or authorization. This had the potential for embarrassment of Patient 4's family if the information was disclosed.

Findings:

During an interview on 8/21/14 at approximately 9:00 AM, the hospital's Privacy Analyst (PA 1) stated that on 8/12/14, when the hospital became aware of the death of Patient 4, the hospital implemented a policy and procedure to monitor all access to Patient 4's EMR. PA 1 stated that within hours of implementing this auditing process, Temp 2 was found to have accessed Patient 4's EMR without business justification or authorization.

PA 1 stated that Temp 2's temporary position at

---

| Event ID: LGNQ11 | 3/24/2015 | 10:02:29AM |

---
the facility was ended on 8/12/14.

PA 1 stated that he and two other hospital representatives, as well as a representative from the agency which provided Temp 2 as a temporary employee, interviewed Temp 2 on 8/14/14. PA 1 reported that during this interview, Temp 2 was very distraught and she apologized to the interviewers for her lapse in judgment when she accessed Patient 4's EMR. PA 1 stated Temp 2 signed a Confidentiality Attestation that she would not disclose any of the information she had seen in Patient 4's EMR.

The hospital provided a copy of the audit performed by the Informational Technology staff. In a letter dated 2/20/15, the Manager of Accreditation and Licensing wrote that the Privacy Department set the parameters of the audit which included Temp 2's name and employee ID, Patient 4's name, date of birth, medical record number, and systems: APEX access which occurred 8/11/14 to present. The letter went on to say that PA 1 reviewed the audit results, in concert with the involved Department Managers, and confirmed that Temp 2 had accessed, without business need or authorization, under the "Module" column, Patient 4's inpatient and outpatient hospital encounters, reports and "Snapshots" (summaries) of protected health information as far back as 1/1/1989.

Record review indicated a copy of the "Confidentiality Attestation" signed by Temp 2 on 8/14/14, in which she agreed not to disclose any of the information she had seen in Patient 4's EMR.

Monitoring:
The Privacy Department has oversight of privacy breaches and takes prompt action to investigate events. The Privacy Department works with the involved parties to ensure an appropriate mitigation has been put in place. This information is reported to the Privacy Compliance Steering Committee quarterly.

Quarterly & Ongoing

Responsible Party:
Chief Privacy Officer

<table>
<thead>
<tr>
<th>(X4) ID</th>
<th>ID</th>
<th>SUMMARY STATEMENT OF DEFICIENCIES</th>
<th>PROVIDER'S PLAN OF CORRECTION</th>
<th>(X5) COMPLETE</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAG</td>
<td>PREFIX</td>
<td>(EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LSC IDENTIFYING INFORMATION)</td>
<td>(EACH CORRECTIVE ACTION SHOULD BE CROSS-REFERENCES TO THE APPROPRIATE DEFICIENCY)</td>
<td>DATE</td>
</tr>
</tbody>
</table>
and acknowledging that she was still bound to respect Patient 4's right to privacy based on her Hospital Confidentiality Statement, and state and federal laws.

Record review indicated Temp 2 had received training of the hospital's "Confidentiality of Patient, Employee and Universal Business Information" policy which she signed on 4/28/14.

Record review indicated a letter, dated 8/19/14, to Patient 4's family notifying them of this breach of medical information.

The facility failed to ensure the confidentiality of Protected Health Information when a temporary staff member accessed Patient 4's electronic medical record without authorization and without business justification. Temp 2's action to access the patient's medical information for improper purposes violated Health and Safety Code 1280.15 and is therefore subject to the applicable civil penalty assessment.

Health and Safety Code 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."

Please see the Plan of Correction detailed in the section referencing 1280.15 (a)
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.

T22 DIV5 CH1 ART7-70707(b)(8) Patients' Rights

(b) A list of these patients' rights shall be posted in both Spanish and English in appropriate places within the hospital so that such rights may be read by patients. This list shall include but not be limited to the patients' rights to:

(8) Confidential treatment of all communications and records pertaining to the care and the stay in the hospital. Written permission shall be obtained before the medical records can be made available to anyone not directly concerned with the care.

This RULE: is not met as evidenced by:

Based on interview and record review, the hospital failed to protect the confidentiality of Patient 4's protected health information (PHI) when a staff member, Temp 2, intentionally accessed Patient 4's electronic medical record (EMR) without business justification or authorization. This had the potential for embarrassment of Patient 4's family if the information was disclosed.

Findings:

<table>
<thead>
<tr>
<th>Event ID: LGNQ11</th>
<th>3/24/2015 10:02:29AM</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDPH L&amp;C</td>
<td>JUL 03 2019</td>
</tr>
<tr>
<td>SAN FRANCISCO DO</td>
<td></td>
</tr>
</tbody>
</table>
Please see details at Health and Safety Code 1280.15 (a).