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

Complaint Intake Number:
CA00389732 - Substantiated

Representing the Department of Public Health:
Surveyor ID # 15727, REHS, HFE I

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 132023. 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.

A. How the correction will be accomplished, both temporarily and permanently. What immediate measures and systemic changes will be put in place to ensure that the deficient practice does not recur.

The involved employee(s) were immediately counseled by Management upon confirmation of the breach. Employment suspension was issued for a period of 3 days for all 3 employees. Review of Privacy Policy & Procedures mandated prior to return to work.

An all staff memorandum was published to communicate Safeguards and HIPAA Privacy Compliance

B. The title or position of the person responsible for correction.

Embedded New Hire Orientation Training revised to elaborate on Privacy and Security Risks specifically around employee snooping.

The Director of Medical Nursing Services along with the Director of Respiratory Care with assistance by Human Resources were responsible for the Written Disciplinary Employment Suspension.

The Privacy Coordinator was responsible for the issuing the all employee memorandum regarding employee snooping.

Event ID: HOCU11
3/29/2016 3:05:14PM

Signature of the principal complainant:

William J. H. Stotuck, Chief Compliance & Risk Officer

Date: 4/1/14
(Employee 1, 2 and 3) accessed Patient 1’s electronic medical record without authorization or a legitimate reason to do so.

Findings:

An unannounced visit was made at the facility on June 10, 2014 to conduct an investigation of a breach of confidentiality of a medical record involving three facility employees unlawfully accessing a coworker’s electronic medical record without authorization.

During an interview on June 10, 2014, at 8:55 a.m., the privacy and compliance coordinator stated three employees accessed the medical record of Patient 1.

A review of the Patient Information Sheet indicated Patient 1 was admitted to the facility on February 15, 2014 with a diagnosis of chest pain.

The “Fair Warning” audit conducted by the facility indicated the following:

Employee 1 accessed Patient 1’s medical record information without a legitimate reason to do so on February 15, February 16 and February 17, 2014. Employee 1 explained that a co-worker told her Patient 1 was admitted to the hospital. Out of concern for the patient, he went into Patient 1’s record to “check in” on her on 3 separate occasions. Employee 1 stated his intentions were good and did not realize this was a breach in privacy.

---

<table>
<thead>
<tr>
<th>(X4) ID PREFIX TAG</th>
<th>ID PREFIX TAG</th>
<th>PROVIDER’S PLAN OF CORRECTION (EACH CORRECTIVE ACTION SHOULD BE CROSS-REFERRED TO THE APPROPRIATE DEFICIENCY)</th>
<th>(X5) COMPLETE DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>The Chief Compliance and Risk Officer was responsible for altering the New Hire Presentation materials and for providing this training 1-2 times monthly to new hires.</td>
<td>08/01/2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Privacy Coordinator attended a one week training course on Fairwarnings to enhance specificity of monitoring access.</td>
<td>05/03/2015</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C. Plan for continued compliance and description of the monitoring process to prevent recurrence of the deficiency; and Date the immediate correction of the deficiency will be accomplished</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Upgraded rules of Fairwarning to better capture those employees who are patients &amp; need additional controls and oversight of access by other employees.</td>
<td>07/01/2015</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ongoing Environment of Care Rounding’s by the Privacy Coordinator will randomly audit compliance of Safeguards and HIPAA Privacy Compliance.</td>
<td>3/13/2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ongoing User Activity by the Privacy Coordinator will randomly audit compliance of Confidentiality Computer Agreements.</td>
<td>03/13/2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mandatory completion of annual educational training which includes topics on “HIPAA Privacy and Security Safeguards”.</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100% compliance achieved with the completion of the annual “Educational Day” Swank Learning Module in 2014 &amp; 2015. Currently at 99.50% for 2016.</td>
<td></td>
</tr>
</tbody>
</table>
Employee 2, who also accessed Patient 1's medical record information without a legitimate reason to do so on February 15, 2014, stated she had gone into the system to find the room number of Patient 1 after learning from Patient 1 that she was admitted to the hospital. Patient 1 had contacted Employee 2 personally and requested her to visit her.

Employee 3 stated she checked Patient 1's chart. She had visited Patient 1 on February 15, 2014 and learned her blood pressure was high. On February 16, 2014, she checked Patient 1's chart to see if she was doing better.

A review of the Confidentiality, Computer Usage and Accountability Agreement indicated Employee 1 signed the document on March 19, 2013. According to that document, employees of the hospital agree to only use confidential information (e.g. medical record information) as needed to perform their legitimate duties as an employee receiving information from the hospital, only access confidential information for which they need to know and not misuse confidential information or carelessly care for confidential information.

The document titled, Confidentiality and Disclosure of Patient Information Agreement for Employee 2 indicated the employee signed the document on May 13, 2008.

The document titled, Confidentiality and Disclosure of Patient Information Agreement for Employee 3 indicated the employee signed the document on August 8, 2013.
indicated the employee signed the document, however did not date the form. The New Employee Orientation Checklist dated November 12, 2007 and signed by Employee 3 on November 12, 2007 included HIPAA (Health Insurance Portability and Accountability Act).

A review of the facility’s report to the Department dated February 28, 2014 indicated, "three employees did inappropriately access their coworker’s electronic health record." The report also indicated, "The documents viewed contained the patient’s name, date of birth, medical record number, account number and clinical information."

Based on the findings, the facility failed to prevent access of medical information of one patient, by three employees, without authorization or a legitimate reason to do so, in violation of Health and Safety Code Section 1280.15(a).