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

Complaint Intake Number: CA00393317 - Substantiated

Representing the Department of Public Health:
Surveyor ID # 15932, Health Facilities Eval.
Nurse

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 58.05 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.

Health and safety code 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. For purposes of this section, internal paper records, electronic mail, or facsimile transmissions inadvertently misdirected within the same facility or health care system within the course of coordinating care or delivering services shall not constitute unauthorized access to, or use or disclosure of a patient's medical information. 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 in this section and other related state and federal statutes and regulations, the extent of 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 whether to investigate the amount of an administrative penalty, if any, pursuant to this section.

T22 DIV5 CH7 ART6-70751 (b) Medical Record Availability

The medical record, including X-ray films, is the property of the hospital and is maintained for the benefit of the patient, the medical staff and the hospital. The hospital shall safeguard the information in the record against loss, defacement, tampering or use by unauthorized persons.

This RULE: is not met as evidenced by:

Based on interview and record review, the facility failed to ensure a registered nurse (RN 1) followed the facility's policy to safeguard patient, PHI (protected health information) when RN 1 copied PHI for 637 (six hundred and thirty seven) patients to an unsecured device. As a result of this violation, the PHI of 637 patients placed on an unsecured, unauthorized device by RN 1, was put at risk when stolen from the front seat of her car parked in her driveway.

Findings:

On 3/28/14, the Department of Public Health (Department) was notified via fax by the
6. Palomar Health procedure "Mobile/Portable and Removable Storage Device Access and Appropriate Usage Standards" # 38212 and associated User Agreement was updated.

7. The User Agreement was redesigned to become an electronic attestation for workforce members to review and sign annually. This attestation verifies that the workforce member is aware of the policies and procedures for safeguarding patient PHI with using Palomar Health Mobile/Portable and Removable Storage Devices.

8. Encrypted Removable Storage Devices will be provided on a need only basis. The devices will be automatically wiped clean if not activated in the time frames identified in procedure 38212.

Monitoring:
1. 20 Random audits will be conducted every month beginning July 2015 for next 4 months to ensure portable storage device data ports are disconnected.

2. Distribution of the encrypted removable storage devices will be monitored by Information Security.
whose data had been breached and identifying information. The Department used the spreadsheet to determine that of the 5,499 patients listed, the breach of PHI affected 637 patients. Specifically, the PHI on the flash drives included names, diagnoses, treatments, and medications of the 637 affected patients.

The DIT provided the facility policy, revised 4/12, titled Computer Systems Usage at (Facility). According to the policy, "Employee and authorized non-employees are responsible to follow PC (personal computer)/Laptop and Portable Device Access and Appropriate Usage Standards procedure as applicable."

According to the facility policy, dated 1/5/12, titled PC/Laptop and Portable Device Access and Appropriate Usage, "Always use shared network drives to store confidential or sensitive data..." and, "Laptops should never be left unattended in a vehicle."

The DIT stated the prohibited use of flash drives was also reviewed in the facility Annual Safety Competencies. In addition, she stated staff could not pass the Annual Safety Exam until they had correctly answered the question related to the use of flash drives.

The PO was interviewed on 4/8/14 at 11:15 A.M. The PO provided the Annual Safety Competencies completed by RN 1 for 2/2009, 2/2010, 2/2011, 2/2012, 2/2013 and 1/2014. The PO also stated the Privacy Office did not
give RN 1 permission to take patient PHI home.

RN 1 was interviewed on 4/8/14 at 12:50 P.M. According to RN 1, she left the two flash drives, along with a facility issued computer laptop, in her work bag on the floor of her car, parked in her driveway overnight. RN 1 stated when she came out to her car the next morning on 2/22/14 at 5:45 A.M., the workbag was missing.

According to RN 1, she had been the Nursing Informatics Manager since October 2011. RN 1 stated as Nurse Informatics Manager, she would download various reports to include medication compliance reports and chart audits. In addition, she downloaded emails with PHI to unencrypted (a process of encoding information in such a way that only authorized parties can read it) personal flash drives without permission from the Privacy Officer. RN 1 stated she did not tell anyone she downloaded patient PHI to her flash drive. RN 1 acknowledged it was, “inappropriate” for her to copy patient PHI to her flash drive saying, “I didn’t connect the dots.”

According to RN 1, she began copying information to one flash drive five years ago, but when that flash drive stopped working properly, “I made a copy of the old one to a new one.” RN 1 stated she kept the broken flash drive which contained patient PHI because, “I didn’t know what to do with it.” She further stated she did not seek advice from her Supervisor or Information Technology
department because, "It didn't cross my mind." RN 1 stated she did not secure the two flash drives in her office because she traveled to all three health care facilities.

As a result of the failure of RN 1 to adhere to the policies and procedures of the facility regarding the protection of medical records, the PHI for 637 patients was placed at an avoidable risk for theft and loss.

<table>
<thead>
<tr>
<th>(X4) ID PREFIX TAG</th>
<th>SUMMARY STATEMENT OF DEFICIENCIES (EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LEC IDENTIFYING INFORMATION)</th>
<th>ID PREFIX TAG</th>
<th>PROVIDER'S PLAN OF CORRECTION (EACH CORRECTIVE ACTION SHOULD BE CROSS-REFERENCED TO THE APPROPRIATE DEFICIENCY)</th>
<th>(X5) COMPLETE DATE</th>
</tr>
</thead>
</table>

Event ID:J15511
8/5/2015 9:19:37AM