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

Complaint Intake Number.
CA00306519 - Substantiated

Representing the Department of Public Health Surveyor ID # 27945. 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...
Continued From page 1

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.

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.

Based on interview and document review, the facility failed to prevent the unauthorized access by Business Staff B to the medical records of four patients on 3/14/12 (Patients 1, 2, 3 and 4)

Findings:

During an interview on 5/10/12 at 3 pm,
Continued From page 2

Administrative Staff A (Admin) verified that she had reported to the Department on 4/12/11 at 2:14 pm, the unauthorized access to the private health information (PHI) of Patients 1, 2, 3 and 4 by Business Staff (Bus Staff) B. Admin Staff A stated the facility became aware of the breach during a routine audit conducted on 4/9/12 at 9:57 am. Bus Staff B had accessed all four patients' electronic medical records on 3/14/12 starting at 1:53 pm and ending at 1:58 pm. He used his own login and password to access the records. Admin Staff A confirmed that all four patients were Bus Staff B's relatives, and that they had been notified by certified letter on 4/12/12 at 3 pm.

On 5/10/12, copies of the computer searches (query search) on 4/14/12 made by Bus Staff B for Patients 1, 2, 3 and 4 were reviewed. During this period, Bus Staff B made one search each for Patients 1, 2, 3 and 4 in the facility's computerized patient information filing system (Meditech). The information accessed by Bus Staff B included Patients 1, 2, 3 and 4 and their demographics including their name, date of birth, physician's name, allergies, physician's orders, lab results, vital signs, diagnoses and various nursing assessments.

The facility's policy, "Corrective Process for Breach," dated 4/10/12 was reviewed. The policy defined a "Breach of Patient Privacy or Confidentiality" occurred when any staff member accessed or reviewed PHI for any reason and not necessary to the employee's role in the provision of care and treatment. The policy also indicated a breach had occurred when any staff

Event ID MRWRG11 1/29/2012

LABORATORY DIRECTOR'S OR PROVIDER/ SUPPLIER REPRESENTATIVE'S SIGNATURE

STATEMENT OF DEFICIENCIES AND PLAN OF CORRECTION

XII PROVIDER/SUPPLIER REASON FOR SURVEY

DEPARTMENT OF PUBLIC HEALTH

CALIFORNIA HEALTH AND HUMAN SERVICES AGENCY

STATEMENT

Sierra Nevada Memorial Hospital

STREET ADDRESS, CITY, STATE, ZIP CODE

155 Glasson Way, Grass Valley, CA 95445-5723 NEVADA COUNTY

SUMMARY STATEMENT OF DEFICIENCIES

(marked with an asterisk *) denotes a deficiency which the institution may be accused of correcting providing it is determined that other safeguards provide sufficient protection to the patients. Except for nursing homes, the findings above are 30 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 30 days following the date these documents are made available to the facility. If deficiencies are cited, an approved plan of correction is required to continued program participation.
Continued From page 3

member "discloses any individual's PHI for purposes not related to patient care and treatment."

On 2/27/12, Bus Staff B had signed a facility, "Privacy & Data Security Education Update /HIPAA Training Acknowledgement Form" certifying that, "I have read and understand this Acknowledgement Form and hereby agree to fully comply with it."

On 5/10/12 at 4:30 pm, Admin Staff A verified that on 3/14/12, Bus Staff B's access to Patients 1, 2, 3 and 4's PHI was unauthorized and that Patients 1, 2, 3 and 4 had not given Bus Staff B authorization to view their records.

The File Clerk was terminated on 4/12/12 for unauthorized access to electronic medical records.

Ongoing: Every new SNMH employee completes New Hire Orientation which includes education on HIPAA and Dignity Health Privacy & Data Security Policies.

Anually, every employee completes mandatory training on HIPAA and Dignity Health Privacy & Data Security Policies.