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

Complaint Intake Number:
CA00289915 - Substantiated

Representing the Department of Public Health
Surveyor ID # 22707, 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, 1723, or 1745 shall prevent unlawful or unauthorized access to, and use or disclosure of patients medical information, as defined in subdivision (g) of Section 5606 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 patient's medical information.

For purposes of the investigation the department shall consider the clinic's, health facility's,

The parent of the patient whose results were accessed inappropriately was notified by the FRH Privacy Official and an apology extended on behalf of the organization.

Laboratory staff were instructed verbally and by e-mail by the Office Lead to complete an event report any time they become aware of a potential privacy breach. They were also instructed to notify their supervisor and the FRH Privacy Official immediately so that appropriate action and notification can occur.

The Laboratory Director has conducted disciplinary action with the staff involved. This individual no longer works at FRH.
### Summary Statement of Deficiencies

**ID Provider/Supplier (CLIA):** 050225

**Type of Construction:** Building B Wing

**Date Survey Completed:** 03/06/2012

### Name of Provider/Supplier

Feather River Hospital

5974 Pentz Rd, Paradise, CA 95969-5509

BUTTE COUNTY

### ID Provider's Plan of Correction

**Prefix:** 

**Tag:** 

**ID:** 

**Provider's Plan of Correction:** The Laboratory Director has required all Laboratory staff to re-sign the organization's confidentiality statement as part of education on privacy provided during a staff meeting. Those not present (on leave) signed upon returning to work. 

**Date:** 11/30/11

**Prefix:** 

**Tag:** 

**ID:** 

**Provider's Plan of Correction:** Confirmation of understanding of the education and effectiveness of requiring staff to re-sign the confidentiality statement will be monitored via the event reporting process that is used to report all suspected privacy breaches. 

**Date:** 12/2/11

### Event Summary

Event ID: X2Y11

4/2/2013 11:10:45AM

**Findings:**

The CDPH verified that the facility failed to inform 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 record review, the facility failed to protect confidential health information for one patient (Patient 1). 

### Agency's History

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 failed to inform 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 record review, the facility failed to protect confidential health information for one patient (Patient 1).
On 11/30/11 at 1 pm, the facility's privacy officer stated that on 11/11 at 8:30 pm, Laboratory Staff 1 (LS 1) gained unauthorized access to Patient 1's medical information and shared the information with her coworkers. The privacy officer stated that LS 1 had accessed Patient 1's name and admitting diagnosis. Patient 1 was the 2 year old son of a phlebotomist supervisor.

On 11/30/11 at 1:30 pm, the Laboratory Director (LD) 2 recalled that LS 1 had been caught by Phlebotomy Supervisor (PS) 3 on 11/11 at 8:30 pm viewing a computer screen displaying a software program called PowerChart. The computer screen listed patients and diagnoses that LS 1 had been previously warned by supervisory staff not to view. LD 2 stated that LS 1 had been directed only to look patients up individually and not access full page screens with patient lists. He stated that LS 1 conducted an Internet search to learn more about Patient 1's diagnosis after obtaining the diagnosis from the PowerChart which she freely shared with her coworkers.

On 11/30/11, the computer screen (PowerChart) used by LS 1 was reviewed. The screen contained the name, room, bed, date of birth, account number, length of stay, physician, medical record number, admission date, admitting diagnosis, and age of multiple patients. LD 2 stated the number of patients visible would depend on the census for the unit chosen; however, LS 1 had only been interested in Patient 1's name and diagnosis at the time of the breach discovery.
During a telephone interview on 3/6/12 at 11:05 am, LD 2 stated that LS 1 accessed the computer screen that had lists of patients and their diagnoses. It was not a computer site that LS 1 would normally use or would need to access in her daily job routine. No other lab personnel had access to this screen/site. LD 2 explained that a former lab director had given LS 1 permission at that time. He explained that the site access could not be removed from LS 1's computer because the facility's software computer system had no way of deleting it.

During an interview on 3/6/12 at 1 pm, LD 2 stated the only time a lab employee would have permission to go into the site that LS 1 accessed would be if he was instructed to do so by himself (lab director) or a supervisor. At that time, it would only be to search for a definitive individual name. Otherwise, LD 2 stated "The lab employees are not allowed to access this site-period."

During a telephone interview on 3/6/12 at 5:40 pm, PS 3 stated she saw LS 1 access the computer screen that showed the names and diagnoses of all patients in the hospital. PS 3 stated she informed LS 1 that she should not be accessing that site. PS 3 stated LS 1 had told her that another supervisor's son (Patient 1) was in the hospital and asked her what his diagnosis meant. PS 3 stated she told LS 1 that she did not know what the diagnosis was and again informed LS 1 that she should not be looking at patients' names and diagnoses. PS 3 stated she saw LS 1 use the computer's Internet site that defined Patient 1's.
PS 3 stated she had been a relatively new supervisor at that time of the breach and was unsure of what the protocol was and what to do about LS 1 being seen on the prohibited site. PS 3 stated she reported the breached information incident to LD 2 at the next supervisor meeting on 11/9/11, a month later.