STATEMENT OF DEFICIENCIES AND PLAN OF CORRECTION

(X1) PROVIDER/SUPPLIER/CUA IDENTIFICATION NUMBER: 050228

(X2) MULTIPLE CONSTRUCTION
A. BUILDING
B. WING

(X3) DATE OF SURVEY COMPLETED 12/23/2009

NAME OF PROVIDER OR SUPPLIER STREET ADDRESS, CITY, STATE, ZIP CODE
SAN FRANCISCO GENERAL HOSPITAL 1001 Potrero Ave, San Francisco, CA 94110-3518 SAN FRANCISCO COUNTY

(X4) ID PREFIX TAG

SUMMARY STATEMENT OF DEFICIENCIES
(EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LSC IDENTIFYING INFORMATION)

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

Complaint Intake Number: CA00211950 - Substantiated

Representing the Department of Public Health:
Surveyor ID # 23107, 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 CA00211950 violation of Health and Safety Code 1280.15(a) for failure to prevent unauthorized access to patients medical information:

Event ID: Y71G11 8/24/2012 11:39:56AM

LABORATORY DIRECTOR'S OR PROVIDER/SUPPLIER REPRESENTATIVE'S SIGNATURE
Susan A. Curry MS
CEO

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 patients. 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.
Informed Medical Breach

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.

1280.15(a) Health & Safety Code 1280

(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
Continued From page 1  

Substantiated.

Informed Medical Breach

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.

1280.15(a) Health & Safety Code 1280

(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

DPH) and of all employees of the University of California, San Francisco (UCSF) who received care as patients at the hospital (emergency department, clinics, acute care, skilled nursing) to verify if the LCR access was appropriate; the total number of audits conducted per month average between 25-30. Questionable audit results are investigated with the manager and employee and action taken as indicated by the investigation. Audit results are reported quarterly to the Privacy Committee.

The SFGH Privacy Officer and the SFGH Privacy Analyst conduct audits of the Lifetime Clinical Record (LCR) of any patient as requested by managers to verify if the LCR access was appropriate, e.g., media high profile cases, VIPs. Questionable audit results are investigated with the manager and employee and action taken as indicated by the investigation. Audit results are reported quarterly to the Privacy Committee.

The SFGH Privacy Officer and the CHN Senior Information Systems Manager present an annual report regarding privacy issues to the SFGH Quality Council. In addition, they report any incidents of non-compliance with DPH and SFGH privacy policies which occur during the year at the next scheduled SFGH Quality Council.

Responsible Person(s):
SFGH Privacy Officer
CHN Senior Information Systems Manager

<table>
<thead>
<tr>
<th>Event ID: Y71G11</th>
<th>8/24/2012 11:39:56AM</th>
<th>LABORATORY DIRECTOR'S OR PROVIDER/SUPPLIER REPRESENTATIVE'S SIGNATURE</th>
<th>TITLE</th>
</tr>
</thead>
</table>

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 patients. 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.
Continued from page 2

($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 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.

T22 DIVS CH1 ART7-70751(b) Medical Record Availability

(b) 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.

These regulations were not met as evidenced by:

Based on interview and record review, the facility failed to protect the medical records of five patients (Patient 1, 2, 3, 4 & 5) from loss and use by unauthorized persons when Physician 1 removed copies of part of the records from the facility. Physician 1's briefcase containing the patients' medical information was stolen from his car on 12/9/09.
Findings:

During an interview on 12/22/09 at 3:10 p.m., Staff A (director of regulatory affairs) stated Physician 1 took copies of Patient 1, 2, 3, 4 & 5's initial infectious disease consultation forms home on 12/29. The forms had the patient's name, medical record number, date of birth, a synopsis of the patient's condition and notations regarding the consultation. Staff A said someone broke into Physician 1's house and stole the briefcase containing the records from his unlocked car in the garage. Staff A stated Physician 1 was "Not supposed to take medical records home."

Staff A said the facility became aware of the incident on 12/30. The Department was notified on 12/30 and a letter of notification was mailed to Patient 1, 2, 3, 4 & 5 on 12/30.

A review of the facility's Health Information Services: Confidentiality, Security, and Release of Protected Health Information policy indicated the following:

Purpose
The purpose of this policy is to ensure:

The confidentiality of protected health information;

Procedure
D. ... They (medical records) must not be taken from (name of facility) premises for any reason.

The SFGH multidisciplinary Privacy Committee, composed of the SFGH Privacy Officer and staff from the SFGH Privacy Office, the SFGH Chief Medical Officer, the SFGH Chief Communications Officer, representatives from the SFGH Legal Affairs, Regulatory Affairs, Health Information Systems departments, as well as representatives from both the SFGH and UCSF Risk Management and Information Systems Departments, meets monthly to review, discuss, and recommend policy involving privacy compliance issues.

In follow-up to a review of facility-related privacy breach cases reported to CDPH conducted by the SFGH Privacy Officer with SFGH managers at the monthly Management Forum meeting, including this 2009 incident, the SFGH Chief of Staff and SFGH Privacy Officer presented the same review to the Chiefs of Service at a Medical Executive Committee (MEC), reminding the chiefs about the hospital and SFDPH privacy and security policies prohibiting the removal of patient protected information (PHI), including copies of the paper medical record, from the hospital, as well as the penalties for violating these policies and the penalties for violating provisions of SB541 and AB211 (see Attachments 2).
## Findings:

During an interview on 12/22/09 at 3:10 p.m., Staff A (director of regulatory affairs) stated Physician 1 took copies of Patient 1, 2, 3, 4 & 5’s initial infectious disease consultation forms home on 12/09. The forms had the patient’s name, medical record number, date of birth, a synopsis of the patient’s condition and notations regarding the consultation. Staff A said someone broke into Physician 1’s house and stole the briefcase containing the records from his unlocked car in the garage. Staff A stated Physician 1 was “Not supposed to take medical records home.”

Staff A said the facility became aware of the incident on 12/22/09. The Department was notified on 12/22/09 and a letter of notification was mailed to Patient 1, 2, 3, 4 & 5 on 12/22/09.

A review of the facility’s Health Information Services: Confidentiality, Security, and Release of Protected Health Information policy indicated the following:

**Purpose**

The purpose of this policy is to ensure:

- The confidentiality of protected health information;

**Procedure**

D. ... They (medical records) must not be taken from (name of facility) premises for any reason.

### Monitoring:

The SFGH Privacy Officer and the SFGH Privacy Analyst conduct monthly audits of the *Lifetime Clinical Record (LCR)* of all employees of the City & County of San Francisco Department of Public Health (CCSF DPH) and of all employees of the University of California, San Francisco (UCSF) who received care as patients at the hospital (emergency department, clinics, acute care, skilled nursing) to verify if the LCR access was appropriate; the total number of audits conducted per month average between 25-30. Questionable audit results are investigated with the manager and employee and action taken as indicated by the investigation. Audit results are reported quarterly to the Privacy Committee.

The SFGH Privacy Officer and the SFGH Privacy Analyst conduct audits of the *Lifetime Clinical Record (LCR)* of any patient as requested by managers to verify if the LCR access was appropriate, e.g., media high profile cases, VIPs. Questionable audit results are investigated with the manager and employee and action taken as indicated by the investigation. Audit results are reported quarterly to the Privacy Committee.
Physician 1 failed to follow the facility’s Health Information Services: Confidentiality, Security, and Release of Protected Health Information policy when he removed protected health information from the facility. The information was later stolen from Physician 1’s car.

The employee’s removal of patient records from the hospital and the subsequent theft of those records from the employee’s home violated Health and Safety Code 1280.15, making the hospital subject to the applicable civil money penalty assessment.

The SFGH Privacy Officer and the CHN Senior Information Systems Manager present an annual report regarding privacy issues to the SFGH Quality Council. In addition, they report any incidents of non-compliance with DPH and SFGH privacy policies which occur during the year at the next scheduled SFGH Quality Council.

Responsible Person(s):
SFGH Privacy Officer
CHN Senior Information Systems Manager

<table>
<thead>
<tr>
<th>Event ID: Y71G11</th>
<th>8/24/2012 11:39:56 AM</th>
</tr>
</thead>
<tbody>
<tr>
<td>LABORATORY DIRECTOR'S OR PROVIDER/SUPPLIER REPRESENTATIVE'S SIGNATURE</td>
<td>TITLE</td>
</tr>
</tbody>
</table>

Any deficiency statement ending with an asterisk (*) denotes a deficiency which the institution may be excused from correcting provided it is determined that other safeguards provide sufficient protection to the patients. 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.