## STATEMENT OF DEFICIENCIES AND PLAN OF CORRECTION

### NAME OF PROVIDER OR SUPPLIER
STANFORD HOSPITAL

### STREET ADDRESS, CITY, STATE, ZIP
300 PASTEUR DRIVE
STANFORD, CA 94305

### (A) PROVIDER/SUPPLIER IDENTIFICATION NUMBER
CA070001357

### (B) BUILDING:
B, WING

### (C) DATE SURVEY COMPLETED
08/14/2013

---

<table>
<thead>
<tr>
<th>ID</th>
<th>SUMMARY STATEMENT OF DEFICIENCIES</th>
<th>ID</th>
<th>PROVIDER'S PLAN OF CORRECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>A001</td>
<td>Informed Medical Breach</td>
<td>A001</td>
<td>Preparation and/or execution of this plan of correction does not constitute admission or agreement by the provider of the truth of the facts alleged or conclusions set forth on the Statement of Deficiencies. This plan of correction is prepared and/or executed solely because it is required by state law.</td>
</tr>
</tbody>
</table>

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.

### A000 Initial Comment

The following reflects the findings of the California Department of Public Health during the investigation of an entity reported incident conducted on 7/30/13 through 8/14/13.

For Entity Reported Incident CA00355653 regarding State Monitoring, Privacy Breach, a State deficiency was identified (see California Health and Safety Code, 1280.15(a)).

Inspection was limited to the entity reported incident investigated and does not represent the findings of a full inspection of the hospital.

Representing the California Department of Public Health: 25438, Health Facilities Evaluator Nurse.
California Department of Public Health

STATEMENT OF DEFICIENCIES AND PLAN OF CORRECTION

<table>
<thead>
<tr>
<th>(X1) PROVIDER/SUPPLIER/CLA IDENTIFICATION NUMBER:</th>
<th>(X2) MULTIPLE CONSTRUCTION</th>
<th>(X3) DATE SURVEY COMPLETED</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA070001357</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NAME OF PROVIDER OR SUPPLIER: STANFORD HOSPITAL
STREET ADDRESS, CITY, STATE, ZIP CODE: 300 PASTEUR DRIVE
STANFORD, CA 94305

<table>
<thead>
<tr>
<th>(X4) ID</th>
<th>PRETEXT</th>
<th>TAG</th>
<th>SUMMARY STATEMENT OF DEFICIENCIES (EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LSO IDENTIFYING INFORMATION)</th>
<th>(X5) ID</th>
<th>PRETEXT</th>
<th>TAG</th>
<th>PROVIDER'S PLAN OF CORRECTION (EACH CORRECTIVE ACTION SHOULD BE CROSS-REFERENCED TO THE APPROPRIATE DEFICIENCY)</th>
<th>(X6) COMPLETE DATE</th>
</tr>
</thead>
</table>
| A-017   |         |     | Continued From page 1                                                                          | A-017   |         |     | which was confirmed in a telephone call to law enforcement on February 21, 2014. No one has contacted the hospital or law enforcement regarding this incident. In an abundance of caution, the patient was promptly notified of the incident and the hospital is unaware of any harm caused to the patient as a result of this incident. Contrary to policies, procedures and training, a resident physician failed to protect patient information in his possession. The vehicle containing the backpack was vandalized and the backpack and other possessions were stolen. The backpack was likely stolen for potential items of monetary value and therefore it is likely that the thief discarded the papers in the backpack, as law enforcement has indicated is typical in such

This Statute is not met as evidenced by:
Based on interview and record review, the hospital failed to prevent unauthorized access to one patient's (Patient 1) medical information.

Findings:
On 5/22/13, the California Department of Public Health received a faxed report from the hospital chief privacy officer which indicated the hospital identified unauthorized access to Patient 1's health information.

During an interview on 7/30/13 at 11:00 a.m., the privacy director stated the hospital was informed on 5/20/13, a backpack which contained 27 pages of Patient 1's medical record was stolen from Physician A's car while it was parked near his home.

Record review on 8/1/13 at 9:30 a.m. indicated Physician A had completed annual privacy training on 5/15/12 and 5/19/13. Record review of the annual Graduate Medical Education policy indicated DO NOT leave patient information or devices containing patient information in a car, a car truck, an unlocked room, or any other area unattended (not even for a few minutes).

During an interview on 8/14/13 at 8:10 a.m., Physician A stated he brought pages of Patient 1's clinical record to present the case before a group of physicians. Physician A stated instead of his usual practice of returning the record to the hospital, he placed it in his backpack which was stolen from his car between midnight and 6:00 a.m. the next day. Physician A stated the information included Patient 1's name, date of birth, medical record number, address and telephone number, insurance information, medical history, treating physician and plan of care. Physician A stated as soon as he was aware of the missing backpack, he contacted the hospital and filed a police report.

Incidents. Other items of value were taken from the vehicle. After conducting a thorough investigation, it is not reasonably expected that unauthorized or inappropriate access to, view or reviewing of medical information occurred.

The hospital Privacy Office immediately launched a complete and thorough investigation into the reported theft.

The following safeguards were in place prior to the incident.

Policies:

- HIPAA: Internal Access to Protected Health Information: V.B.3. "Workforce members or departments maintaining paper files, lists, or any documents containing PHI are responsible for securely maintaining and storing that information as long as needed.
<table>
<thead>
<tr>
<th>ID PREFIX</th>
<th>TAG</th>
<th>SUMMARY STATEMENT OF DEFICIENCIES (EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LIC IDENTIFYING INFORMATION)</th>
<th>ID PREFIX</th>
<th>TAG</th>
<th>PROVIDER'S PLAN OF CORRECTION (EACH CORRECTION ACTION SHOULD BE CROSS-REFERENCED TO THE APPROPRIATE DEFICIENCY)</th>
<th>COMPLETE DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A017</td>
<td></td>
<td>and shredding or securely disposing of it when no longer needed.</td>
<td>A017</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HIPAA: Internal Access to Protected Health Information: V.B.4.</td>
<td></td>
<td></td>
<td>“Workforce members receiving PHI are responsible for ensuring that the information is safeguarded while in their possession.”</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>“When a user prints information from a hospital information system, the user is responsible for handling patient information confidentially, protecting it from unauthorized secondary disclosure, and shredding or returning to HIMS when the use is completed.”</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Resident Physician Policy and Procedure: “DO NOT leave patient information or devices containing patient information in a car, a car trunk, unlocked room, or any other area</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>SUMMARY STATEMENT OF DEFICIENCIES</td>
<td>DEFICIENCY ID</td>
<td>PLAN OF CORRECTION</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>----------------------------------</td>
<td>---------------</td>
<td>-------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| A017 | unattended (not even for a few minutes).” | A017 | (For the purposes of this policy, “Corrective Action” means sanctions/disciplinary action.) “Taking patient information off premises and failing to protect that information.” (Offense for which sanctions will be applied.)

Physician-focused training:
- Privacy and Security presentations for various physician groups.
- Email to Residents and Clinical Fellows from the School of Medicine Associate Dean, Undergraduate and Graduate Medical Education, on Patient Privacy Protection with reminders of steps that should be taken and steps that should be avoided when considering access, use, or transmittal of patient information.
**STATEMENT OF DEFICIENCIES AND PLAN OF CORRECTION**

<table>
<thead>
<tr>
<th>Identification Number</th>
<th>Provider/Supplier/CLA</th>
<th>Multiple Construction</th>
<th>Date Survey Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA070001357</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NAME OF PROVIDER OR SUPPLIER**

STANFORD HOSPITAL
300 PASTEUR DRIVE
STANFORD, CA 94305

**SUMMARY STATEMENT OF DEFICIENCIES**

<table>
<thead>
<tr>
<th>ID PREFIX TAG</th>
<th>ID PREFIX TAG</th>
</tr>
</thead>
<tbody>
<tr>
<td>A017</td>
<td>A017</td>
</tr>
</tbody>
</table>

- Annual mandatory training on Privacy and Security policies and safeguards.

**Awareness Reminders:**

- November 15, 2011: The Dean of the School of Medicine published a newsletter article regarding privacy and security protections for patients and the institution.
- December 2012, within a broader privacy and security awareness campaign, a specific awareness poster was posted throughout the hospital, “Think your Car Is Safe? Don’t leave valuables in your car or your trunk. Take your valuables with you.”

**Plan of Correction:**

The hospital proactively protects the confidentiality and privacy of all patient information and provides training to workforce members.
California Department of Public Health

STATEMENT OF DEFICIENCIES AND PLAN OF CORRECTION

<table>
<thead>
<tr>
<th>ID PREFIX TAG</th>
<th>SUMMARY STATEMENT OF DEFICIENCIES</th>
<th>ID PREFIX TAG</th>
<th>PROVIDER'S PLAN OF CORRECTION</th>
</tr>
</thead>
</table>
| A017          |                                   | A017          | on its privacy policies. In a continual effort to improve its Privacy Assurance Program, the provider will review its existing policies and procedural controls that pertain to safeguards for protection of paper documents containing patient information and will continue to issue periodic reminders and awareness posters specific to the protection of paper information and not leaving patient information in vehicles. 

For patients affected by the incident

The provider notified the one patient in an abundance of caution, as mentioned above. The patient was provided with a contact name and number to call the provider with any questions. To date, the patient has not contacted the hospital with questions or concerns and the hospital is unaware of any harm caused the patient by the incident. | 05/07/2013 |
<table>
<thead>
<tr>
<th>ID</th>
<th>SUMMARY STATEMENT OF DEFICIENCIES (EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LSO IDENTIFYING INFORMATION)</th>
<th>PROVIDER'S PLAN OF CORRECTION (EACH CORRECTIVE ACTION SHOULD BE CROSS-REFERENCED TO THE APPROPRIATE DEFICIENCY)</th>
<th>COMPLETION DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A017</td>
<td>For other patients having the potential to be affected by a similar incident</td>
<td>The provider continually seeks opportunities to strengthen its privacy and information security programs for the protection of the medical information of the patients it serves. Immediate measures were taken as follows:</td>
<td></td>
</tr>
</tbody>
</table>
A. As a result of the resident physician's violation of policies and training, appropriate disciplinary action was imposed. [May, 2013]

B. The resident physician attested to his understanding of resident physician policies and procedures which specifically state “DO NOT leave patient information or devices containing patient information in a car, a car trunk, an unlocked room, or any other area unattended (not even for a few minutes).” [May, 2013]

C. As part of the ongoing program, workforce members are required to complete privacy and security training online. 
   a) Immediately re-trained the resident physician [May 19, 2013]
   b) Retrained the workforce using updated training [August, 2013]

D. Within 45 days after the incident, the School of Medicine and the hospital
E. The School of Medicine MD Program Handbook and Policy Manual, Academic Year 2013-2014, was updated and included the policy, "Privacy and Security Protection for the Removal and Transport of Protected Health Information."

F. Stanford Physician leadership communicated staff reminders on provider policies emphasizing requirements for strong safeguards to protect papers in their possession that contain patient information.
NAME OF PROVIDER OR SUPPLIER: STANFORD HOSPITAL
STREET ADDRESS, CITY, STATE, ZIP CODE: 300 PASTEUR DRIVE, STANFORD, CA 94305

<table>
<thead>
<tr>
<th>ID PREFIX TAG</th>
<th>SUMMARY STATEMENT OF DEFICIENCIES (EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LSC IDENTIFYING INFORMATION)</th>
<th>ID PREFIX TAG</th>
<th>PROVIDER'S PLAN OF CORRECTION (EACH CORRECTION ACTION SHOULD BE CROSS-REFERENCED TO THE APPROPRIATE DEFICIENCY)</th>
<th>COMPLETE DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A017</td>
<td></td>
<td>A017</td>
<td>G. Hospital-wide Privacy Awareness Campaigns in 2013 and 2014 included specific information reinforcing policy safeguards not to leave PHI in cars. Monitoring performance to ensure corrections are achieved and sustained (Revised March 5, 2014) 1. Upon registration of each new patient, the location of the patient's medical record will be documented on a log. 2. Any physician and/or resident that will be presenting the patient's information at the Cancer Center Head &amp; Neck Tumor Board the same day will need to sign the log and attest to returning the paper chart by close of business the same day. The paper chart will not leave the building.</td>
<td></td>
</tr>
</tbody>
</table>
3. The log will be monitored by the Clinic Management and any discrepancies immediately reported, Administrative Director of Cancer Care Program and the Cancer Center Quality Committee.

4. Individuals that are not compliant with the policy will be reported to the Cancer Center Administration.

5. The monitoring of paper records will remain effective until such time that an electronic solution can be implemented.

6. A report of the monitoring results will be submitted to the Privacy Governance Council.