### Background

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.

The hospital did not report to the California Department of Public Health (CDPH) that a Breach of patient health information occurred. Rather, the hospital, in an abundance of caution, notified CDPH within five business days of a "possible" Incident under Health and Safety Code Section 1280.15. In an abundance of caution, the patient was promptly notified of the incident; however, over a year and a half later, the patient has not complained of any harm.

### Initial Comment

The following reflects the findings of the California Department of Public Health during the Investigation of an entity reported incident conducted from 8/18/14 to 10/20/14.

For Entity Reported Incident CA00349367, regarding State Monitoring. Privacy Breach to entities outside hospital (one State deficiency was identified (see California Health and Safety Code, Section 1280.15(a)).

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

Representing the California Department of Public Health: 32398, Health Facilities Evaluator Nurse.

<table>
<thead>
<tr>
<th>ID</th>
<th>PREFIX TAG</th>
<th>ID</th>
<th>PREFIX TAG</th>
<th>COMPLETE DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A 001</td>
<td>Informed Medical Breach</td>
<td>A 001</td>
<td>Background</td>
<td></td>
</tr>
<tr>
<td>Health and Safety Code Section 1280.15 (b)(2), &quot;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.&quot;</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>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The hospital did not report to the California Department of Public Health (CDPH) that a Breach of patient health information occurred. Rather, the hospital, in an abundance of caution, notified CDPH within five business days of a "possible" Incident under Health and Safety Code Section 1280.15. In an abundance of caution, the patient was promptly notified of the incident; however, over a year and a half later, the patient has not complained of any harm.
The hospital detected the Breach of Patient's Health Information (PHI) on 3/25/13. The hospital reported the Breach of PHI to the Department on 4/1/13. The hospital notified Patient 1 of the Breach of PHI on 4/1/13.

There remains no evidence of actual inappropriate access to, use or disclosure of the patient's health information to date. The hospital's thorough investigation revealed that a single email, which was inadvertently misdirected, was recalled expeditiously and then promptly deleted from the server at the hospital's direction. The email was sent after normal business hours for those on the recipient list, significantly decreasing the likelihood of access. The limited claim information mostly demographic was contained in an attachment (not the email itself), which also significantly reduced the likelihood of access, especially for a recalled email. The possible recipients were other health care providers and vendors who are legally obligated to protect the confidentiality of patient information.

<table>
<thead>
<tr>
<th>ID</th>
<th>PREFIX</th>
<th>TAG</th>
<th>SUMMARY STATEMENT OF DEFICIENCIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>A000</td>
<td></td>
<td></td>
<td>Continued From page 1</td>
</tr>
<tr>
<td>A017</td>
<td>1280.15(a)</td>
<td>Health &amp; Safety Code 1280</td>
<td></td>
</tr>
</tbody>
</table>

(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 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.
This Statute is not met as evidenced by: Based on interview and record review, the hospital failed to prevent the unauthorized disclosure of patient health information (PHI) for one of one sampled patient (1), when a pediatric patient's (Patient 1) claim form was inadvertently emailed to a group distribution list. The failure resulted in the disclosure of Patient 1's PHI to unauthorized entities. Findings:

The California Department of Public Health received a faxed report on 4/1/13, which indicated, on 3/27/13 a single claim form which contained Patient 1's name, address, telephone number, insurance name and identification number, diagnosis code, date of birth, and provider, was inadvertently emailed to a group distribution list.

During an interview on 8/18/14 at 2:45 p.m., the compliance and privacy officer (CPO) stated a pharmacy senior account representative (SAR) inadvertently emailed Patient 1's claim form on 3/25/13 to a Listserv. The CPO stated the SAR was having problems filling out the claim form, so she had telephoned the vendor of the software program which fills out claim forms. The vendor had asked the SAR to email him the claim form. The SAR inadvertently emailed the claim form to the vendor's Listserv of about 1,026 health care facilities. The CPO stated the hospital's IT security staff recalled the emailed message "right away", but the CPO was not sure how many were actually recalled. The CPO stated the hospital did not have a copy of the claim form. The CPO stated the claim form disclosed Patient 1's name, address, telephone number, insurance name and
### Summary Statement of Deficiencies

Based on interview and record review, the hospital failed to prevent the unauthorized disclosure of patient health information (PHI) for one of one sampled patient (1), when a pediatric patient's (Patient 1) claim form was inadvertently emailed to a group distribution list. The failure resulted in the disclosure of Patient 1's PHI to unauthorized entities. Findings:

The California Department of Public Health received a faxed report on 4/1/13, which indicated, on 3/27/13 a single claim form which contained Patient 1's name, address, telephone number, insurance name and identification number, diagnosis code, date of birth, and provider, was inadvertently emailed to a group distribution list.

During an interview on 8/18/14 at 2:45 p.m., the compliance and privacy officer (CPO) stated a pharmacy senior account representative (SAR) inadvertently emailed Patient 1's claim form on 3/25/13 to a Listserve. The CPO stated the SAR was having problems filling out the claim form, so she had telephoned the vendor of the software program which fills out claim forms. The vendor had asked the SAR to email him the claim form. The SAR inadvertently emailed the claim form to the vendor's Listserve of about 1,026 health care facilities. The CPO stated the hospital's IT security staff recalled the emailed message "right away", but the CPO was not sure how many were actually recalled. The CPO stated the hospital did not have a copy of the claim form. The CPO stated the claim form disclosed Patient 1's name, address, telephone number, insurance name and

### Corrective Action

Contrary to policies, procedures and training, the SAR failed to protect patient information in her possession. The SAR did not adhere to policy and training that require special precautions be taken when sending email information containing PHI nor did SAR adhere to policies and training that require application of the minimum necessary standard. While this was an isolated incident, the hospital applied its corrective action policy to prevent recurrence.

### Policies

**HIPAA Security: Electronic Mail Policy**

III. "It is the policy of Lucille Packard Children's Hospital at Stanford to provide electronic mail to its workforce members to facilitate communications within and outside SHC, with reasonable security controls to ensure confidentiality of ePHI and other sensitive SHC data."
This Statute is not met as evidenced by:
Based on interview and record review, the hospital failed to prevent the unauthorized disclosure of patient health information (PHI) for one of one sampled patient (1), when a pediatric patient's (Patient 1) claim form was inadvertently emailed to a group distribution list. The failure resulted in the disclosure of Patient 1's PHI to unauthorized entities. Findings:

The California Department of Public Health received a faxed report on 4/1/13, which indicated, on 3/27/13 a single claim form which contained Patient 1's name, address, telephone number, insurance name and identification number, diagnosis code, date of birth, and provider, was inadvertently emailed to a group distribution list.

During an interview on 8/18/14 at 2:45 p.m., the compliance and privacy officer (CPO) stated a pharmacy senior account representative (SAR) inadvertently emailed Patient 1's claim form on 3/25/13 to a Listserve. The CPO stated the SAR was having problems filling out the claim form, so she had telephoned the vendor of the software program which fills out claim forms. The vendor had asked the SAR to email him the claim form. The SAR inadvertently emailed the claim form to the vendor's Listserve of about 1,026 health care facilities. The CPO stated the hospital's IT security staff recalled the emailed message "right away", but the CPO was not sure how many were actually recalled. The CPO stated the hospital did not have a copy of the claim form. The CPO stated the claim form disclosed Patient 1's name, address, telephone number, insurance name and

HIPAA: Use and Disclosure of Protected Health Information

F. "When using or disclosing PHI, or requesting PHI from another covered entity, SHC/LPCH will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The minimum necessary requirement does not apply to certain uses or disclosures, including those authorized by the individual and those needed by a healthcare provider for treatment purposes."

HIPAA: Internal Access to Protected Health Information

V.E.1. "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."
This Statute is not met as evidenced by: Based on interview and record review, the hospital failed to prevent the unauthorized disclosure of patient health information (PHI) for one of one sampled patient (1), when a pediatric patient's (Patient 1) claim form was inadvertently emailed to a group distribution list. The failure resulted in the disclosure of Patient 1's PHI to unauthorized entities. Findings:

The California Department of Public Health received a faxed report on 4/1/13, which indicated, on 3/27/13 a single claim form which contained Patient 1's name, address, telephone number, insurance name and identification number, diagnosis code, date of birth, and provider, was inadvertently emailed to a group distribution list.

During an interview on 8/18/14 at 2:45 p.m., the compliance and privacy officer (CPO) stated a pharmacy senior account representative (SAR) inadvertently emailed Patient 1's claim form on 3/25/13 to a Listserve. The CPO stated the SAR was having problems filling out the claim form, so she had telephoned the vendor of the software program which fills out claim forms. The vendor had asked the SAR to email him the claim form. The SAR inadvertently emailed the claim form to the vendor's Listserve of about 1,026 health care facilities. The CPO stated the hospital's IT security staff recalled the emailed message "right away", but the CPO was not sure how many were actually recalled. The CPO stated the hospital did not have a copy of the claim form. The CPO stated the claim form disclosed Patient 1's name, address, telephone number, insurance name and number, diagnosis code, date of birth, and provider.

Policy: Confidentiality Statement

"I understand that I am responsible for protecting PHI or medical information that is sent by me via facsimile and/or electronically such as e-mail and I am responsible for following the applicable policies with respect to the transmission of PHI or medical information and that any inappropriate disclosure of information may make me subject to legal and/or disciplinary action."

Since the patient information was contained in an attachment to the email, and the email was recalled quickly on an evening, after recipients' normal work hours we are not aware that any of the unintended recipients actually accessed the information.

A single patient claim information was inadvertently emailed as an attachment to the email. There was no patient information in the body of the email. The employee immediately contacted hospital's IT
<table>
<thead>
<tr>
<th>(X4) ID</th>
<th>SUMMARY STATEMENT OF DEFICIENCIES (EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LSC IDENTIFYING INFORMATION)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A017</td>
<td>Continued From page 3 Identification number, diagnosis code, date of birth, and provider.</td>
</tr>
</tbody>
</table>

During an interview on 10/20/14 at 9 a.m., SAR stated, at about 4:30 p.m. she was helping a coworker with a claim form. SAR stated she was on the telephone with the vendor of the software program which produces the claim forms, and the vendor had remote access to her computer. SAR stated the claim form was not printing correctly so the vendor asked SAR to email the printed claim form to him. SAR stated the vendor did not receive the claim form after she emailed it, and they realized the form was inadvertently emailed to the vendor's Listserve. SAR stated she recalled the email within 30 minutes of sending the email. SAR stated the vendor company was located on the East Coast and was on Eastern Standard Time (EST) (which would have been 7:30 p.m., end of business day). SAR stated most of the entities on the vendor's Listserve were located on the East Coast and most likely did not open the email. SAR stated about 99% of the emails were probably recalled, but the hospital was not able to locate the actual number which were recalled.

A review of a copy of a letter, which the CPO stated was sent on 4/1/13, from the hospital to Patient 1's family member indicated on 3/27/13 the hospital's privacy office was made aware on 3/25/13 a claim form with Patient 1's name address and telephone number, insurance name and Identification number, diagnosis code, date of birth, and provider disclosed was inadvertently emailed to a group distribution list.

Several requests to review a copy of the hospital's policy regarding electronic mailing of Patient Health Information was submitted.

<table>
<thead>
<tr>
<th>ID</th>
<th>SECURITY FOLLOWED INSTRUCTIONS TO RECALL THE EMAIL AND IN THE INTERIM, SENT AN EMAIL INSTRUCTING RECipients TO DELETE THE EMAIL. THE LATTER WAS SENT WITHIN 21 MINUTES, AND THE RECALL OCCURRED WITHIN APPROXIMATELY 45 MINUTES. THE HOSPITAL WAS IN THE PROCESS OF PERMISSIBLY RESPONDING TO A VENDOR, UNDER CONFIDENTIALITY AGREEMENT WITH THE HOSPITAL, FOR TROUBLESHOOTING SUPPORT, WHEN THE EMAIL WAS INADVERTENTLY MISDIRECTED TO THE VENDOR'S LISTSERVE. ACCORDING TO THE HOSPITAL'S VENDOR, THERE WERE NOT 1,026 HEALTH CARE FACILITIES ACTIVELY PARTICIPATING IN THE LISTSERVE DURING THE PERIOD WHEN THIS OCCURRED TWENTY MONTHS AGO. RATHER, THE VENDOR STATED THAT IT HAD 600 ACTIVE MEMBERS GENERALLY, BUT DID NOT HAVE A RECORD THAT ANY ACCESSED THE ATTACHMENT TO THE EMAIL AT ISSUE.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A017</td>
<td>Security and followed instructions to recall the email and in the interim, sent an email instructing recipients to delete the email. The latter was sent within 21 minutes, and the recall occurred within approximately 45 minutes. The hospital was in the process of permissibly responding to a vendor, under confidentiality agreement with the hospital, for troubleshooting support, when the email was inadvertently misdirected to the vendor's listserv. According to the hospital's vendor, there were not 1,026 health care facilities actively participating in the listserv during the period when this occurred twenty months ago. Rather, the vendor stated that it had 600 active members generally, but did not have a record that any accessed the attachment to the email at issue.</td>
</tr>
</tbody>
</table>
A017 Continued From page 4

However, the hospital did not provide a copy of the policy regarding electronic mailing of Patient Health Information.

A017

The CPO does not recall being asked for the claim form. The hospital has the claim form and can provide upon request. Regarding the question as to how many emails were recalled, the employee immediately contacted hospital's IT Security and received instruction to recall the email and accomplished this within 45 minutes, which gave rise to a good faith belief by the hospital that all or nearly all emails were recalled.

The hospital CPO verbally provided relevant policy references. The hospital has had longstanding policy on electronic mailing of PHI, and offers to provide the policy as support for the previously provided references.
## Summary Statement of Deficiencies

**ID** | **Prefix** | **Tag** | **Provider's Plan of Correction** (Each corrective action should be cross-referenced to the appropriate deficiency) | **Complete Date**
---|---|---|---|---
A017 | Continued From page 4 | A017 | **Plan of Correction**

**For the patient affected by the incident**

The provider notified the patient who was affected by this incident. The patient was provided with a contact name and number to call the provider with any questions. The patient has not contacted the hospital or otherwise expressed any concerns.

**For other patients having the potential to be affected by a similar incident**

This was an isolated incident and limited to the one employee who failed to follow policy and double-check that the appropriate e-mail address was selected to prevent the email from going to unintended recipients. The employee was sanctioned and was re-trained to prevent recurrence of a similar incident.

---

**State Form**

CALIFORNIA DEPARTMENT OF PUBLIC HEALTH

FEB 12 2015

L & C DIVISION

SAN JOSE
A017 Continued From page 4

However, the hospital did not provide a copy of the policy regarding electronic mailing of Patient Health Information.

A 017

Immediate measures and enhancements to prevent recurrence

The hospital 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:

a. Within twenty minutes of sending the original email attachment, the employee sent a second email to all recipients directing them to immediately delete the email and attachment.

b. Within thirty minutes of sending the original email, the employee worked with IT security to recall the original email. Recalling the message removes the message from anyone's inbox who has not already opened the message. The SAR confirmed the effectiveness of the recall because
<table>
<thead>
<tr>
<th>ID PREFIX</th>
<th>TAG</th>
<th>SUMMARY STATEMENT OF DEFICIENCIES</th>
<th>PROVIDER'S PLAN OF CORRECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>A 017</td>
<td></td>
<td>Continued From page 4</td>
<td></td>
</tr>
</tbody>
</table>

However, the hospital did not provide a copy of the policy regarding electronic mailing of Patient Health Information.

She in fact received the email indicating her original email had been recalled. The provider's vendor is located on the east coast and the majority of the vendor's clients are also located on the east coast. The original email with attachment was sent well after normal business hours. The hospital has a good faith belief that all or nearly all of the unintended recipients would not have had the opportunity to open the email and open the claim attachment prior to its recall. According to the hospital's vendor, although the listserv was comprised of 1,029 members, only 600 of those members were active listserv members in general, for purposes of reading software updates; there is no evidence that any listserv member opened this attachment or viewed limited medical information.
NAME OF PROVIDER OR SUPPLIER: LUCILE SALTER PACKARD CHILDREN'S HOSPITAL
STREET ADDRESS, CITY, STATE, ZIP CODE: 725 WELCH ROAD, PALO ALTO, CA 94304

SUMMARY STATEMENT OF DEFICIENCIES (EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LSO IDENTIFYING INFORMATION) Continued From page 4

However, the hospital did not provide a copy of the policy regarding electronic mailing of Patient Health Information.

c. The hospital's vendor confirmed that the original email was removed from its server.

d. Hospital workforce members are required to complete mandatory Privacy training annually, pass a competency test and complete an attestation statement acknowledging their responsibility to comply with Privacy policies and procedures.

Monitoring performance to ensure corrections are achieved and sustained.

i. The hospital will continue evaluative and preventative efforts on PHI data transmissions which will be reported to the hospital Director of IT Security for a period of one year from the date of incident.
California Department of Public Health

STATEMENT OF DEFICIENCIES
AND PLAN OF CORRECTION

(A) PROVIDER/SUPPLIER/CLA.
IDENTIFICATION NUMBER:

CA070001349

(B) MULTIPLE CONSTRUCTION
A. BUILDING: ___________________________

C. WING: __________________________

(C) DATE SURVEY COMPLETED

C

10/20/2014

NAME OF PROVIDER OR SUPPLIER
LUCILE SALTER PACKARD CHILDREN'S HOSP.

STREET ADDRESS, CITY, STATE, ZIP CODE
725 WELCH ROAD
PALO ALTO, CA 94304

(D) ID PREFIX

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

ID
PREFIX

TAG

A 017
Continued From page 4

However, the hospital did not provide a copy of
the policy regarding electronic mailing of Patient
Health Information.

A 017

Hospital's functional
manager over pharmacy
claims processing functions
will monitor employee
actions related to emailing
claims information to
Hospital's business
associate vendors for a
period of one year from
the date of incident.

March 27,
2014

March 27,
2014

December
2014

March 27,
2014

iv. Hospital will include in its
annual 2015 privacy
awareness campaign,
specific mention for
employee's to double-
check the recipient in the
"To" line of each email.

iv. Hospital will include in its
annual 2015 privacy
awareness campaign,
California Department of Public Health

STATEMENT OF DEFICIENCIES AND PLAN OF CORRECTION

<table>
<thead>
<tr>
<th>(X1) PROVIDER/SUPPLIER/Cler</th>
<th>(XS) MULTIPLE CONSTRUCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA070001349</td>
<td>A. BUILDING:</td>
</tr>
<tr>
<td></td>
<td>B. WING:</td>
</tr>
<tr>
<td></td>
<td>C. COMPLETED</td>
</tr>
</tbody>
</table>

NAME OF PROVIDER OR SUPPLIER: LUCILE SALTER PACKARD CHILDREN'S HOSPITAL
STREET ADDRESS, CITY, STATE, ZIP CODE: 725 WELCH ROAD, PALO ALTO, CA 94304

NAME OF PROVIDER OR SUPPLIER: LUCILE SALTER PACKARD CHILDREN'S HOSPITAL
STREET ADDRESS, CITY, STATE, ZIP CODE: 725 WELCH ROAD, PALO ALTO, CA 94304

SUMMARY STATEMENT OF DEFICIENCIES PROVIDER'S PLAN OF CORRECTION

<table>
<thead>
<tr>
<th>(X4) ID</th>
<th>PREFIX TAG</th>
<th>SUMMARY STATEMENT OF DEFICIENCIES</th>
<th>PROVIDER'S PLAN OF CORRECTION</th>
<th>COMPLETED DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A017</td>
<td></td>
<td>Continued From page 4</td>
<td>A017</td>
<td>December 2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>However, the hospital did not provide a copy of the policy regarding electronic mailing of Patient Health Information.</td>
<td>A. A report of monitoring results will be submitted to the Privacy Governance Council.</td>
<td></td>
</tr>
</tbody>
</table>

CALIFORNIA DEPARTMENT OF PUBLIC HEALTH

FEB 12 2015
L & C DIVISION
SAN JOSE