POC Accepted 6.4.10 11:43AM - Talked to Tonya Okon K-Sullivan

PRINTED: 04/23/2010
FORM APPROVED

California Department of Public Health

STATEMENT OF DEFICIENCIES AND PLAN OF CORRECTION	(X1) PROVIDER/SUPPLIER/CLIA IDENTIFICATION NUMBER:	(X2) MULTIPLE CONSTRUCTION	(X3) DATE SURVEY COMPLETED
	CA070001349	A. BUILDING _____ B. WING _____	C 03/24/2010

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

CALIFORNIA DEPARTMENT OF PUBLIC HEALTH
JUN 11 2010
LICENSING & CERTIFICATION DIVISION
SAN JOSE

(X4) ID PREFIX TAG	SUMMARY STATEMENT OF DEFICIENCIES (EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LSC IDENTIFYING INFORMATION)	ID PREFIX TAG	PROVIDER'S PLAN OF CORRECTION (EACH CORRECTIVE ACTION SHOULD BE CROSS-REFERENCED TO THE APPROPRIATE DEFICIENCY)	(X5) COMPLETE DATE
A 000	Initial Comment The following reflects the findings of the California Department of Public Health during investigation of two entity reported incidents conducted on March 24, 2010. For Entity Reported Incident CA00219273, regarding retention of a foreign object in a patient, the Department was unable to identify a violation of State or Federal regulations. For Entity Reported Incident CA00219008, regarding a breach of protective health information, State deficiencies were identified (see California Code of Regulations, Title 22, Section 70707(b)(8), and Health and Safety Code, Sections 1280(b)(1) and 1280(b)(2)). Inspection was limited to the specific entity reported incidents investigated and does not represent the findings of a full inspection of the hospital. Representing the California Department of Public Health was Kathleen Sullivan, Health Facilities Evaluator Nurse.	A 000	**ENTITY REPORTED INCIDENT CA00219008** **A000** **NOTE REGARDING PLAN OF CORRECTION** 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. Further, the provider disputes the determination made by DPH and has requested a hearing under Health and Safety Code section 131071. **Background** **A000, A018, A019, E1953** On 2/1/10, the provider determined that medical information for 532 patients was on the hard drive of a desktop computer that was reported as having been stolen by the same employee to whom the computer and the information contained in it had been assigned and used for performance of legitimate work duties. From 2/2/10 to 2/16/10, the Palo Alto Police Department (PAPD) under the scope of its legal authority conducted an investigation into the theft allegations. Information resulting from the PAPD investigation would be essential to the provider's	
A 018	1280.15(b)(1) Health & Safety Code 1280 (b) (1) A clinic, health facility, agency, or hospice to which subdivision (a) applies shall report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information to the department no later than five days after the unlawful or unauthorized access, use, or disclosure has been detected by the clinic, health facility, agency, or hospice. This Statute is not met as evidenced by:	A 018		

Licensing and Certification Division

Tonya Okon — Director - Privacy Assurance — 6/10/10

LABORATORY DIRECTOR'S OR PROVIDER/SUPPLIER REPRESENTATIVE'S SIGNATURE — TITLE — (X6) DATE

STATEMENT OF DEFICIENCIES AND PLAN OF CORRECTION	(X1) PROVIDER/SUPPLIER/CLIA IDENTIFICATION NUMBER:	(X2) MULTIPLE CONSTRUCTION	(X3) DATE SURVEY COMPLETED
	CA070001349	A. BUILDING _____ B. WING _____	C 03/24/2010

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

(X4) ID PREFIX TAG	SUMMARY STATEMENT OF DEFICIENCIES (EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LSC IDENTIFYING INFORMATION)	ID PREFIX TAG	PROVIDER'S PLAN OF CORRECTION (EACH CORRECTIVE ACTION SHOULD BE CROSS-REFERENCED TO THE APPROPRIATE DEFICIENCY)	(X5) COMPLETE DATE
A 018	Continued From page 1 Based on interviews and record review, the hospital failed to report a privacy breach to the Department within five days after the hospital confirmed a stolen computer contained protected health information (PHI) for 532 patients. Findings: On 3/24/10 at 9:55 a.m. during an interview with the Director of Privacy Assurance (DPA), she stated on 1/11/10 the Director of the Heart Center (DHC) received an e-mail from the Manager of the Heart Center (MHC). The e-mail indicated a computer was removed from the center by an unauthorized employee (Employee 1). The DPA notified Human Resources (HR) on 1/11/10 that Employee 1 was observed removing the computer with the help of her husband (Employee 2). HR notified the privacy office on 1/12/10. The DPA stated the information technology (IT) department performed an analysis of information on the missing computer. The analysis took place from 1/11/10 through 2/1/10. The IT analysis verified Employee 1 moved data from the secure network to unsecured areas on the computer's local drive. During an interview with the human resource employee (HR 1) on 3/24/10 at 11:00 a.m., he stated the MHC speculated in the e-mail dated 1/11/10 to the DHC, there might be PHI on the missing computer. Two hospital employees gave statements they witnessed Employee 1 and Employee 2 remove the computer from the office. During an interview with the DPA on 3/24/10 at	A 018	detection of any unauthorized access, use, or disclosure of the information contained on the computer. Based on the PAPD's conclusion that findings were sufficient to refer the matter to the District Attorney's office, and there was no recovery of the computer to assist in detection efforts as to whether unauthorized access, use, or disclosure of patient medical information occurred, notification efforts to patients and CDPH ensued for the reporting of a *possible* violation of Health & Safety Code section 1280.15(b)(1). Notification to CDPH was done on 2/19/10 in an abundance of caution considering the fact that this desktop computer is enabled with a security tool that notifies the provider if any outside person uses the computer to connect to the Internet. Generally, if an unauthorized person takes a computer, law enforcement often can locate a suspect from monitoring reports of access to the Internet using this type of sophisticated security tool. These reports have been actively monitored and no evidence of usage has been reported. The provider protects the confidentiality of patient medical information and has 26 privacy policies and 27 information security policies in place for the protection of patient medical information and trains its employees to its policies and procedures. Despite solid policies, appropriate safeguards and employee training, criminal activity cannot be 100% deterred. The provider continually seeks opportunities to strengthen its privacy and information security programs for the protection of	

STATEMENT OF DEFICIENCIES AND PLAN OF CORRECTION	(X1) PROVIDER/SUPPLIER/CLIA IDENTIFICATION NUMBER:	(X2) MULTIPLE CONSTRUCTION	(X3) DATE SURVEY COMPLETED
	CA070001349	A. BUILDING _____ B. WING _____	C 03/24/2010

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

(X4) ID PREFIX TAG	SUMMARY STATEMENT OF DEFICIENCIES (EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LSC IDENTIFYING INFORMATION)	ID PREFIX TAG	PROVIDER'S PLAN OF CORRECTION (EACH CORRECTIVE ACTION SHOULD BE CROSS-REFERENCED TO THE APPROPRIATE DEFICIENCY)	(X5) COMPLETE DATE
A 018	Continued From page 2 11:15 a.m., she stated the police were notified on 1/27/10 about the missing computer. Letters were sent on 2/19/10 to the 532 patients who had PHI on the computers. The hospital had three different notification letters based on the different data involved for each patient. The confidential data included names, dates of birth, medical record numbers, diagnoses, procedures, insurance information and/or social security numbers. The hospital reported the incident to the Department on 2/19/10, 19 days after the hospital confirmed the missing computer contained PHI for 532 patients.	A 018	the medical information of the patients it serves. **Plan of Correction** **A018, A019, E1953** *For patients affected by the incident* The provider recognizes that notifications advising patients of an incident that could involve the possibility of access to their medical information by an unauthorized person can be disconcerting to patients and their families. In good faith, the provider at its own expense offered patients affected by this incident support services such as a dedicated toll-free telephone number to get questions answered as well as coverage offerings scaled to the level of potentially compromised data to include medical identity theft restoration services, identity theft coverage, and credit monitoring services. Following coordination of service offerings and activation codes that would enable patients' parents to access these medical/identity theft coverage and credit monitoring services, a notification letter was sent to each patient on 2/26/10 with a unique activation code for each patient inserted and instructions on how to access offered services. *For other patients having the potential to be affected by a similar incident* The provider is strongly committed to ensuring the privacy and security of its patients' information and has an extensive set of existing policies and practices	
A 019	1280.15(b)(2) Health & Safety Code 1280 (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 days after the unlawful or unauthorized access, use, or disclosure has been detected by the clinic, health facility, agency, or hospice. This Statute is not met as evidenced by: Based on interviews and record review, the hospital failed to notify a privacy breach of patients' protected health information (PHI) to 532 patients within five days after the hospital confirmed the breach on 2/1/10. The hospital failed to send notifications to the patients until 2/19/10. Findings: On 3/24/10 at 9:55 a.m. during an interview with the Director of Privacy Assurance (DPA), she stated on 1/11/10 the Director of the Heart Center	A 019		

California Department of Public Health

STATEMENT OF DEFICIENCIES AND PLAN OF CORRECTION	(X1) PROVIDER/SUPPLIER/CLIA IDENTIFICATION NUMBER:	(X2) MULTIPLE CONSTRUCTION	(X3) DATE SURVEY COMPLETED
	CA070001349	A. BUILDING _____ B. WING _____	C 03/24/2010

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

(X4) ID PREFIX TAG	SUMMARY STATEMENT OF DEFICIENCIES (EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LSC IDENTIFYING INFORMATION)	ID PREFIX TAG	PROVIDER'S PLAN OF CORRECTION (EACH CORRECTIVE ACTION SHOULD BE CROSS-REFERENCED TO THE APPROPRIATE DEFICIENCY)	(X5) COMPLETE DATE
A 019	Continued From page 3 (DHC) received an e-mail from the Manager of the Heart Center (MHC). The e-mail indicated a computer was removed from the center by an unauthorized employee (Employee 1). The DPA notified Human Resources (HR) on 1/11/10 that Employee 1 was observed removing the computer with the help of her husband (Employee 2). HR notified the privacy office on 1/12/10. The DPA stated the information technology (IT) department performed an analysis of information on the missing computer. The analysis took place from 1/11/10 through 2/1/10. The IT analysis verified Employee 1 moved data from the secure network to unsecured areas on the computer's local drive. During an interview with the human resource employee (HR 1) on 3/24/10 at 11:00 a.m., he stated the MHC speculated in the e-mail dated 1/11/10 to the DHC, there might be PHI on the missing computer. Two hospital employees gave statements they witnessed Employee 1 and Employee 2 remove the computer from the office. The hospital sent three different notification letters based on the different data involved for each patient. The confidential data included names, dates of birth, medical record numbers, diagnoses, procedures, insurance information and/or social security numbers. On 2/19/10 the notification letters were sent to the 532 patients, 19 days after the hospital confirmed the privacy breach occurred.	A 019	in place. This POC addresses how the provider will further strengthen its protection of data on desktop computers so that even in the unfortunate event of a stolen asset, the risk is further minimized that data on the computer asset is not available, accessible, readable, or decipherable by an unauthorized individual. With respect to notification requirements, this POC addresses how the provider will update its policies to incorporate new statutory provisions related to law enforcement activities and DPH expectations as to when reporting should occur. A. The provider's current policy requires that patient medical information always be saved to secure locations on computers. In addition to data that is available to employees through secure network servers e.g., electronic medical record and clinical systems, employees are provided with secure file space where data saved to these locations are kept secure on the provider's secure network. Employees are trained that saving outside of these secure areas e.g., to the desktop or the computer's hard drive (c: drive) is against policy. When data is saved to secure locations, the risk is minimized that data would be available, accessible, readable, or decipherable by an unauthorized individual. To reinforce this important policy, IT Management will: (1) Retrain staff on the policy. A reminder	

STATEMENT OF DEFICIENCIES AND PLAN OF CORRECTION	(X1) PROVIDER/SUPPLIER/CLIA IDENTIFICATION NUMBER:	(X2) MULTIPLE CONSTRUCTION	(X3) DATE SURVEY COMPLETED
	CA070001349	A. BUILDING _____ B. WING _____	C 03/24/2010

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

(X4) ID PREFIX TAG	SUMMARY STATEMENT OF DEFICIENCIES (EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LSC IDENTIFYING INFORMATION)	ID PREFIX TAG	PROVIDER'S PLAN OF CORRECTION (EACH CORRECTIVE ACTION SHOULD BE CROSS-REFERENCED TO THE APPROPRIATE DEFICIENCY)	(X5) COMPLETE DATE
E1953	Continued From page 4	E1953	notice to all employees was sent on May 12, 2010, as has been done periodically for some time, referencing the policy and specifically calling out the risks associated with storing patient data on local unencrypted workstations as opposed to centrally managed and secured file servers and clinical applications.	May 12, 2010
E1953	T22 DIV5 CH1 ART7-70707(b)(8) Patients' Rights (b) A list of these patients' rights shall be posted in both Spanish and English in appropriate places within the hospital so that such rights may be read by patients. This list shall include but not be limited to the patients' rights to: (8) Confidential treatment of all communications and records pertaining to the care and the stay in the hospital. Written permission shall be obtained before the medical records can be made available to anyone not directly concerned with the care. This Statute is not met as evidenced by: Based on interviews and record review, the hospital failed to protect the patients' rights to confidentiality when an employee placed 532 patients' encrypted medical information to non-protected sites in her computer. The employee removed the computer from the hospital on 1/5/10. Findings: On 3/24/10 at 9:55 a.m. during an interview with the Director of Privacy Assurance (DPA), she stated on 1/11/10 the Director of the Heart Center (DHC) received an e-mail from the Manager of the Heart Center. The e-mail indicated an unauthorized employee (Employee 1) had removed a computer from the center. The DPA notified Human Resources (HR) on 1/11/10 that Employee 1 was observed removing the computer with the help of her husband (Employee 2). HR notified the privacy office on 1/12/10. The DPA stated she began her	E1953	(2) Re-initiate a plain language campaign specific to data storage ensuring that employees understand and have been given a virtual demonstration on (a) the simple steps to take to ensure that a file is saved to a secure space and (b) what it looks like to save to a space that is not secure, with clear indication that the latter practice is prohibited. Communications sent out as part of the plain language campaign will be targeted to all hospital staff.	June 10, 2010
			(3) Continue to focus its on-going evaluative and preventative efforts on computers with clinical applications and computers with assigned users who work with patient medical information as part of their job function. Using existing reports and new audit methodology:	June 10, 2010
			a. Periodically audit a sampling of computers per month to determine if files are saved to spaces other than the hospital's secure network.	

STATEMENT OF DEFICIENCIES AND PLAN OF CORRECTION	(X1) PROVIDER/SUPPLIER/CLIA IDENTIFICATION NUMBER:	(X2) MULTIPLE CONSTRUCTION	(X3) DATE SURVEY COMPLETED
	CA070001349	A. BUILDING _____ B. WING _____	C 03/24/2010

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

(X4) ID PREFIX TAG	SUMMARY STATEMENT OF DEFICIENCIES (EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LSC IDENTIFYING INFORMATION)	ID PREFIX TAG	PROVIDER'S PLAN OF CORRECTION (EACH CORRECTIVE ACTION SHOULD BE CROSS-REFERENCED TO THE APPROPRIATE DEFICIENCY)	(X5) COMPLETE DATE
E1953	Continued From page 5 department's investigation on that date. The DPA stated the information technology (IT) department performed an analysis of information on the missing computer. The analysis took place from 1/11/10 through 2/1/10. The IT analysis verified Employee 1 moved data from the secure network to unsecured areas on the computer's local drive. The IT analysis determined the information was moved by Employee 1 using her access code during scheduled times at work. Employee 1 admitted she and Employee 2 removed the computer from the Heart Center on 1/5/10, took it to a room in another building and locked it there. The hospital was not able to retrieve the computer. The DPA stated over 400 patients' data was moved to the unsecure local drive. A second group of patients, numbering over 50, had data moved which included the previous information, and medical insurance numbers. A third group included six patients whose moved data included all of the previous information, and social security numbers. During an interview with the human resource employee (HR 1) on 3/24/10 at 11:00 a.m., he stated the e-mail from the MHC to the DHC dated 1/11/10, speculated there might be PHI on the missing computer. During the hospital's investigation, two other employees (Employee 3 and Employee 4) gave statements they witnessed Employee 1 remove the computer from the office. During an interview with the DPA on 3/24/10 at 11:15 a.m., she stated the police were notified on 1/27/10 about the missing computer. Letters were	E1953	b. Utilize audit findings for timely feedback, outreach opportunities and proactive education & training for the user assigned to the identified computer and, when needed, the user's department manager. (4) Evaluate technical solutions and tools available in the marketplace for IT Management to proactively and routinely scan, monitor, and detect data that resides outside of secure network space so that proactive steps can be taken with an employee to bring that specific data into a secure area and retrain the employee on policy requirements. *For quality assurance and effectiveness* (1) Continue to provide periodic reminders and training specific to the do's and don'ts described in A(2) above and re-emphasize the specific instructions provided in existing confidentiality agreements that new employees sign. (2) Periodically review and assess audit finding results as referenced in A(3) above to (a) evaluate the effectiveness of the re-education campaign and (b) evaluate the need for additional administrative and technical controls.	June 30, 2010 Periodic and on-going Periodic and on-going

STATEMENT OF DEFICIENCIES AND PLAN OF CORRECTION	(X1) PROVIDER/SUPPLIER/CLIA IDENTIFICATION NUMBER:	(X2) MULTIPLE CONSTRUCTION	(X3) DATE SURVEY COMPLETED
	CA070001349	A. BUILDING _____ B. WING _____	C 03/24/2010

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

(X4) ID PREFIX TAG	SUMMARY STATEMENT OF DEFICIENCIES (EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LSC IDENTIFYING INFORMATION)	ID PREFIX TAG	PROVIDER'S PLAN OF CORRECTION (EACH CORRECTIVE ACTION SHOULD BE CROSS-REFERENCED TO THE APPROPRIATE DEFICIENCY)	(X5) COMPLETE DATE
E1953	Continued From page 6 sent on 2/19/10 to the 532 patients who had PHI on the computers. The hospital sent three different notification letters based on the different patient data breaches. On 3/24/10 a record review of the hospital policy and procedure, "Privacy-Related Complaints, Reporting, and Breach Notification", dated 9/14/09, indicated the hospital was to meet State and Federal breach notification requirements when a violation of privacy was detected or discovered. The hospital privacy office was required upon discovery or detection of a reportable issue, to notify affected patients within five days, and the California Department of Public Health (CDPH) within 5 days.	E1953	(3) Clarification on the timeframe to notify the patient and DPH i.e., 5 business days instead of 5 calendar days following discovery or detection of a reportable issue. *For effectiveness and quality assurance:* (1) The provider will review its breach notification policy periodically, not less frequently than every three years, and revise as necessary to reflect applicable changes in law or regulation. (2) The provider will provide periodic reminders and training to staff on its breach notification policy.	

California Department of Public Health

STATEMENT OF DEFICIENCIES AND PLAN OF CORRECTION	(X1) PROVIDER/SUPPLIER/CLIA IDENTIFICATION NUMBER:	(X2) MULTIPLE CONSTRUCTION	(X3) DATE SURVEY COMPLETED
	CA070001349	A. BUILDING _____ B. WING _____	C 03/24/2010

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

(X4) ID PREFIX TAG	SUMMARY STATEMENT OF DEFICIENCIES (EACH DEFICIENCY MUST BE PRECEDED BY FULL REGULATORY OR LSC IDENTIFYING INFORMATION)	ID PREFIX TAG	PROVIDER'S PLAN OF CORRECTION (EACH CORRECTIVE ACTION SHOULD BE CROSS-REFERENCED TO THE APPROPRIATE DEFICIENCY)	(X5) COMPLETE DATE
E1953	Continued From page 6 sent on 2/19/10 to the 532 patients who had PHI on the computers. The hospital sent three different notification letters based on the different patient data breaches. On 3/24/10 a record review of the hospital policy and procedure, "Privacy-Related Complaints, Reporting, and Breach Notification", dated 9/14/09, indicated the hospital was to meet State and Federal breach notification requirements when a violation of privacy was detected or discovered. The hospital privacy office was required upon discovery or detection of a reportable issue, to notify affected patients within five days, and the California Department of Public Health (CDPH) within 5 days.	E1953	B. The provider will update its breach notification policy to address the following: (1) The new provisions of Health and Safety Code section 1280.15(c)(1) pertaining to law enforcement involvement in a matter where reporting requirements might apply. Specifically, the provider will obtain written confirmation from law enforcement or document a law enforcement officer's oral representation that notifying patients during a law enforcement investigation will impede the investigation and that notification is to be delayed until the conclusion of the law enforcement activity. Delay in notification does not apply to the Statute's requirement for the provider's notification to DPH. (2) The provider, per its policy, is required upon discovery or detection of a reportable issue, to notify patients within five days, and DPH within five days. The provider will review and revise its policy regarding what constitutes a reportable detection of unauthorized access upon changes to or clarification of applicable laws (whether by the legislature, DPH, and/or the judicial system).	June 10, 2010

STANFORD HOSPITAL AND CLINICS

Tonya Okon MBA, CHP
Director, Privacy Assurance.
Office: Stanford Shopping Center, suite V860
180 el Camino Real, Palo Alto, CA 94304
OfficePhone: 650-736-1855
Fax: 650.723-3628

Fax Cover Sheet

DATE: 6/10/2010

TO: Albert Quintero @ CDPH

PHONE: (408) 277-1784
FAX: **(408) 277-1032**

PAGES: 9 (including cover)

RE: Corrected POC for CA00219008

Mr. Quintero,

Please find attached the corrected POC for CA00219008.

Tonya Okon