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 03/18/2013

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 001	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.	A 001	**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. E000, E1953: T22 DIV5, CH1, ART7-70707(b)(8) The provider protects the confidentiality and privacy of all patient records and communications. Workforce members are required to adhere to privacy and security policies pertaining to the protection of patient information, including	
E 000	Initial Comments The following reflects the findings of the California Department of Public Health during the investigation of an entity reported incident conducted on 3/18/13. For Entity Reported Incident CA00339975 regarding State Monitoring, Privacy Breach, a State deficiency was identified (see California Code of Regulations, Title 22, Section 70707(b)(8)). 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.	E 000	information in electronic form. The provider's policies and training specifically state that, "PHI should not be stored on a computer hard drive or any storage devices unless the PHI is encrypted and the device is password protected. Unencrypted PHI should only be stored on network drives that are housed in secure locations." Policy and training further states that computers and portable devices "must be encrypted if you download or store PHI or other sensitive information on them." Policy and training also require workforce members to ensure the security of devices and to not leave devices unattended in vehicles. While the workforce member (Physician A) had legitimate work related access to and use of the patient information for a quality care review/initiative,	Continued

Licensing and Certification Division

LABORATORY DIRECTOR'S OR PROVIDER/SUPPLIER REPRESENTATIVE'S SIGNATURE — TITLE: Chief Compliance Officer — (X6) DATE: 05/03/2013

POC accepted 5/9/13 Tioga, #FEN

PRINTED: 04/18/2013
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 03/18/2013

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 1	E1953	Physician A did not adhere to policy and training that required that no PHI be placed on unencrypted devices nor did Physician A adhere to policies and training that electronic devices not be left unattended in a vehicle. The physician's School of Medicine (SoM) - issued laptop was protected with a strong, complex password consistent with federal National Institute of Standards and Technology (NIST) authentication standards. In addition, the laptop had a security tool installed (BigFix) that enables detection of whether the computer connects to a network such as the Internet. This system has been regularly monitored and no network connection has been observed since the theft. There continues to be no evidence of inappropriate disclosure of information that was on the laptop. **Plan of Correction** *For patients affected by the incident* The provider notified the potentially affected patients in writing and patients were provided with a contact name and number to call the provider with any questions. While the information that was on the computer is not the type that ordinarily poses a risk for identity theft, identity protection services were offered at no cost to potentially affected patients to help mitigate any concern.	1/16/13
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 interview and record review, the hospital failed to implement a patient's right to confidential treatment of their protected information for 57,000 patients. Findings: During an interview on 3/18/13 at 10:30 a.m., the Director of Privacy stated on 1/9/13 a hospital issued laptop computer was stolen from a physician's car. The computer contained protected health information for 57,000 patients of the hospital. The Director of Privacy stated the disclosed information included patient names and medical record numbers, the number of hospital admissions and outpatient visits, and designation of the complexity of the patients conditions. The Director of Privacy stated in some cases, specific medical conditions were included in the breached information. During an interview at 10:50 a.m., the Information Security Officer stated the particular patient	E1953		Continued

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 03/18/2013

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 2 health information disclosed was considered "restricted" and was required to be encrypted. The Information Security Officer stated the information on the computer was not encrypted During an interview at 12:30 p.m., Physician A stated the computer was hospital issued and used for clinical purposes to access medical records, for administrative uses such as e-mails, and grant writing for research projects. Physician A stated he was sent a file with patients' protected health information related to clinical complexity. He opened and reviewed it and saved it to a file on the computer. After a period of time he forgot it was there. Physician A stated on 1/9/13 he left the computer in his locked car concealed under the passenger seat. When he returned, the window was smashed and the computer had been stolen. Physician A stated he reported the incident to the police and to the privacy officer. Record review on 3/19/13 at 3:10 p.m. of the hospital policy "HIPAA (Health Insurance Portability and Accountability Act of 1996) Security: Workstation Use and Placement" dated September 2011 indicated: "Portable Lucile Packard Children's Hospital workstations (e.g. laptops or tablets) must be configured and encrypted to protect any LPCH internal information they may hold."	E1953	Additionally, a dedicated toll-free telephone number was established for communications and questions. *For other patients having the potential to be affected by a similar incident* For other patients having the potential to be affected by a similar incident, the provider reviewed existing policies and procedural controls to see where controls may be enhanced and implemented immediate measures and enhancements (as described below) to prevent recurrence. *Immediate measures and enhancements to prevent recurrence* 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: A. The workforce member was placed on administrative leave following the incident. Upon completion of the investigation and review of corrective action for failure to comply with security policies and training, corrective measures were communicated in writing to the workforce member.	1/16/13 3/15/13 Continued

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 03/18/2013

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 2 health information disclosed was considered "restricted" and was required to be encrypted. The Information Security Officer stated the information on the computer was not encrypted During an interview at 12:30 p.m., Physician A stated the computer was hospital issued and used for clinical purposes to access medical records, for administrative uses such as e-mails, and grant writing for research projects. Physician A stated he was sent a file with patients' protected health information related to clinical complexity. He opened and reviewed it and saved it to a file on the computer. After a period of time he forgot it was there. Physician A stated on 1/9/13 he left the computer in his locked car concealed under the passenger seat. When he returned, the window was smashed and the computer had been stolen. Physician A stated he reported the incident to the police and to the privacy officer. Record review on 3/19/13 at 3:10 p.m. of the hospital policy "HIPAA (Health Insurance Portability and Accountability Act of 1996) Security: Workstation Use and Placement" dated September 2011 indicated: "Portable Lucile Packard Children's Hospital workstations (e.g. laptops or tablets) must be configured and encrypted to protect any LPCH Internal information they may hold."	E1953	B. As part of ongoing training, University employees including SoM workforce members were required to complete a security awareness video. This is in addition to existing privacy and security training. C. Before the incident, there were strong encryption policies and other controls in place to protect electronic patient information. As part of its ongoing comprehensive proactive program, hospital laptops were already encrypted before the incident and a laptop encryption initiative was being completed at the School of Medicine. Additional resources were devoted to completing the initiative and it has been completed. Encryption of new laptops is on-going. D. Enhanced technical mechanisms were initiated to allow IT Security Administrators to check workforce member adherence to encryption policies. Mechanisms would allow IT Security Administrators to have real-time visibility into the encryption status of devices.	3/12/13 On-going 11/1/12 - 3/1/13 Continued

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 03/18/2013

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 2 health information disclosed was considered "restricted" and was required to be encrypted. The Information Security Officer stated the information on the computer was not encrypted During an interview at 12:30 p.m., Physician A stated the computer was hospital issued and used for clinical purposes to access medical records, for administrative uses such as e-mails, and grant writing for research projects. Physician A stated he was sent a file with patients' protected health information related to clinical complexity. He opened and reviewed it and saved it to a file on the computer. After a period of time he forgot it was there. Physician A stated on 1/9/13 he left the computer in his locked car concealed under the passenger seat. When he returned, the window was smashed and the computer had been stolen. Physician A stated he reported the incident to the police and to the privacy officer. Record review on 3/19/13 at 3:10 p.m. of the hospital policy "HIPAA (Health Insurance Portability and Accountability Act of 1996) Security: Workstation Use and Placement" dated September 2011 indicated: "Portable Lucile Packard Children's Hospital workstations (e.g. laptops or tablets) must be configured and encrypted to protect any LPCH Internal information they may hold."	E1953	*Monitoring performance to ensure corrections are achieved and sustained* The Hospital and the School of Medicine (SoM) will continue to focus 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. Information Security Departments will oversee the monitoring. A. Quarterly x2 and periodically thereafter, audit a sampling of computers to determine if files are saved to unsecure locations. i. Periodically review and assess audit findings for timely feedback, outreach opportunities and proactive education and training for the user assigned to the identified computer and, when needed, the user's department manager. ii. Periodically review and assess audit finding results to evaluate the effectiveness of the re-education and evaluate the need for additional administrative and technical controls.	5/17/13; On-going Continued

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 03/18/2013

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 2 health information disclosed was considered "restricted" and was required to be encrypted. The Information Security Officer stated the information on the computer was not encrypted During an interview at 12:30 p.m., Physician A stated the computer was hospital issued and used for clinical purposes to access medical records, for administrative uses such as e-mails, and grant writing for research projects. Physician A stated he was sent a file with patients' protected health information related to clinical complexity. He opened and reviewed it and saved it to a file on the computer. After a period of time he forgot it was there. Physician A stated on 1/9/13 he left the computer in his locked car concealed under the passenger seat. When he returned, the window was smashed and the computer had been stolen. Physician A stated he reported the incident to the police and to the privacy officer. Record review on 3/19/13 at 3:10 p.m. of the hospital policy "HIPAA (Health Insurance Portability and Accountability Act of 1996) Security: Workstation Use and Placement" dated September 2011 indicated: "Portable Lucile Packard Children's Hospital workstations (e.g. laptops or tablets) must be configured and encrypted to protect any LPCH internal information they may hold."	E1953	B. Continue to evaluate the effectiveness of technical solutions and tools to proactively and routinely scan, monitor, and detect data that resides outside of secure network space e.g., unencrypted environment so that proactive steps can be taken with a workforce member to bring that specific data into compliance with provider policies. C. Continue providing periodic reminders and training specific to privacy and security "Do's and Don't's" and re-emphasize specific instructions provided in training that new workforce members sign. D. Continue to evaluate training needs based on monitoring results; E. Implement improvements based on continuous evaluation, as components of a comprehensive privacy and security program. CALIFORNIA DEPARTMENT OF PUBLIC HEALTH MAY - 9 2013 L & C DIVISION SAN JOSE End	