CEDARS-SINAI

September 5, 2014

##A3178-L01-0123456 **********3-DIGIT 159
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Dear Sample A Sample:

Although there is no indication of any actual or attempted unauthorized access to or use of your health information, we are writing to inform you of the theft of a password-protected Cedars-Sinai-issued laptop computer that may have contained certain information relating to you. There is no indication this laptop computer contained your complete medical or billing records.

Cedars-Sinai takes the security of our patients' health information very seriously, and has multiple security safeguards in place to protect health information. Even a potential data security incident on a single computer, as has occurred here, is not acceptable to us. We deeply apologize for this incident, and have taken actions to prevent any re-occurrence.

On June 23, 2014, a Cedars-Sinai employee's home was burglarized, and a Cedars-Sinai-issued laptop computer and personal items of the employee were stolen. This laptop was used by the Cedars-Sinai employee for specific tasks related to troubleshooting software used for clinical laboratory reporting, and this employee's duties included being available outside of normal business hours to troubleshoot software issues as they occurred. The employee reported the theft to both law enforcement and Cedars-Sinai the same day. Law enforcement's investigation is ongoing, no arrests have been made, and the laptop computer has not been recovered.

Cedars-Sinai launched a comprehensive investigation upon learning of the theft to determine whether the laptop computer contained patient health information at the time of the theft. Cedars-Sinai retained independent experts in computer forensics to assist in this investigation. While this investigation is ongoing, we've confirmed certain patient health information was potentially stored in temporary files on the laptop computer's hard drive at the time of the theft. By manually and electronically reviewing the contents of these temporary files, we've confirmed the files contained your Social Security number. These files may have also contained some combination of your name, demographic information, testing/treatment/diagnosis information, health insurance/non-financial billing information, medical record/account number, date of birth, and driver's license number.

0123456

In addition to taking the steps described above, we terminated remote access to our computer network from the stolen device and conducted a review of our internal policies and procedures related to the storage and transmission of protected health information, as well as the enforcement of our employees' adherence to these policies and procedures. We are taking all necessary steps to ensure that this type of event does not occur again in the future.

(OVER PLEASE)

Cedars-Sinai is unaware of any attempted or actual unauthorized access to or misuse of your health information, but has provided information in this letter on additional steps you can take to protect your identity should you feel it is appropriate to do so. We are also providing you access to a **complimentary** one-year membership of Experian's® ProtectMyID® Elite product. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: 11/30/14** (Your code will not work after this date.)
2. Visit the **ProtectMyID Web Site to enroll: http://www.protectmyid.com/enroll**
3. PROVIDE **Your Activation Code: ABCDEFGHIJKL**

If you have questions or need an alternative to enrolling online, please call (877) 441-6943 and provide engagement #: **PC88611.**

Additionally, we have established a confidential assistance line staffed with professionals familiar with this incident and ways to protect against identity theft and fraud. Should you have any questions about this incident or the contents of this letter, or the types of information relating to you that may have been contained in the files, you may contact this confidential assistance line Monday through Friday, 10:00 a.m. to 7:00 p.m., EST at (877) 218-2930. Please use reference number 7388081314 when calling.

Please know that we are taking all appropriate steps to guard against this from happening in the future, and that the safety and security of your patient information remains our highest priority.

Sincerely,

David C. Blake
Vice President, Corporate Integrity Program
Cedars-Sinai Health System

Information About Identity Theft Prevention

As a precaution, we recommend that you regularly review any Explanation of Benefits (EOB) statements that you receive or have received from your health insurer. If you identify services listed on your EOB that you believe you did not receive, please immediately contact the appropriate health insurer.

We also encourage you to review account statements and to monitor credit reports for suspicious activity. Under U.S. law, you are entitled to obtain one free credit report annually from each of the three major credit reporting bureaus, if one exists. To order your free credit report, visit www.annualcreditreport.com or call, toll-free: (877) 322-8228. You may also contact the three major credit bureaus directly to request a free copy of this credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because a fraud alert tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below. Information regarding security freezes is also available from these agencies.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

You can also further educate yourself regarding identity theft, security freezes, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, (877) ID-THEFT ((877) 438-4338); TTY: (866) 653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them, and information regarding fraud alerts and security freezes may also be obtained from the Federal Trade Commission. Instances of known or suspected identity theft should also be reported to law enforcement and/or your state's Attorney General.

For information about medical privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection Unit at www.privacy.ca.gov.

0123456