Keck Medical Center of USC

Hospital Administration
Rodney Hanners
Chief Operating Officer, Keck Medicine of USC
& Chief Executive Officer for Keck Hospitals

September 20, 2016

NOTICE OF DATA BREACH

What Happened?

On August 1st 2016, USC Keck and Norris Hospitals detected ransomware on two servers after being notified earlier that day that certain hospital employees could not access their files. This type of malware attack encrypted files on both servers, which made the files inaccessible to our employees. However, the attack was quickly contained and isolated to prevent the spreading of malware to other servers.

We notified the FBI immediately and began an internal forensic investigation. We also engaged Ernst & Young, LLP to review the steps we took to investigate the matter. Within several days, we were able to remediate the incident and fully restore the data from the encrypted folders to the servers. No ransom was paid.

We are notifying patients because we identified certain sensitive information that was in the folders encrypted by the malware. Our investigation has not revealed any evidence that data was retrieved or accessed as a result of this ransomware. Typically, ransomware is used to deny users access to their information in order to quickly extract money from the data owners - not to steal data. However, as a precaution, we are providing this notice to patients or other individuals whose health or other personal information was in the encrypted folders.

What Information Was Involved?

The impacted servers do not store Keck's electronic medical record system. Rather, many of the folders that were encrypted by the malware are departmental files that contain internal operational documents and that are intended to be used and shared by and among hospital and clinic personnel, such as templates, training manuals, human resource materials and other information needed for hospital operations.

Our investigation is continuing, but to date, we have identified the following categories of documents that had sensitive data and that were encrypted by the malware attack. Sensitive data included name and demographic information, date of birth, identifiable health information, including treatment and diagnosis for some patients, and in certain cases, social security numbers.

Hospital Administration
Rodney Hanners
Chief Operating Officer, Keck Medicine of USC
& Chief Executive Officer for Keck Hospitals

- Outpatient hospital clinic patients that submitted a request to release health information between July 27, 2015 and August 1, 2016. These documents contained social security numbers where the patient requesting the release of records had provided it.
- Residents and preceptors that participated in the Department of Family Medicine's former residency program from 1999 to 2008. Some of these files contained social security numbers for departmental purposes, such as to pay stipends.
- Patients of the La Canada-Flintridge clinic between August 1, 2011 and August 1, 2016. These files contained documents such as encounter forms and billing summaries, but did not contain social security numbers or other sensitive financial data.

We also located legacy files for the Family Medicine department, which contained spreadsheets with health information consisting of physician name, medical record number, and dates of service, insurance plan and CPT code, dated July 2009. The spreadsheets did not include name, other identifiable information or sensitive financial data.

What We Are Doing:

As a result of this incident, we are working diligently to further improve our security detection and response processes. For example, we are enhancing our audit and logging capabilities so that we can quickly detect and respond to potential threats, including ransomware malware. We already had invested in additional tools to identify malicious traffic but accelerated implementation of those technologies. Further, we are exploring the use of technologies that will protect data at rest through appropriate encryption services.

In addition, we are beginning a process to review all of the folders on these servers to either delete documents that we no longer need to retain or further secure those files with sensitive data that should be retained.

We notified the California Department of Public Health and are notifying the California Attorney General and the U.S. Department of Health and Human Services' Office for Civil Rights of this incident.

Hospital Administration
Rodney Hanners
Chief Operating Officer, Keck Medicine of USC
& Chief Executive Officer for Keck Hospitals

What You Can Do:

It is important to reiterate that there is no evidence that data was retrieved or accessed as a result of this ransomware attack and therefore, we have no reason to believe your information was used in an improper way. However, we also want to make you aware of certain precautionary measures that you might consider. These measures are good practices regardless of this incident and even if you have not identified any suspicious activity related to your accounts.

You should carefully check all credit card and other financial account information that you receive. If you detect any unauthorized or suspicious activity in any of these accounts, you should contact your credit card company or other account issuer immediately.

We recommend that you place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days. You can place a 90 day fraud alert through any of the reporting agencies listed below.

Equifax
800.525.6285
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

Experian
888.397.3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

TransUnion
800.680.7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834
www.transunion.com

We also recommend that you obtain a credit report from one of the three credit bureaus; Experian, Equifax or TransUnion. You can do so at: www.annualcreditreport.com. Following such reviews, you should promptly report any suspicious activity to the proper law enforcement authorities including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC") at www.ftc.gov.

In addition, USC Keck and Norris Hospitals have arranged to offer free credit monitoring and other identity recovery services through ID Experts for one year for the individuals identified above.

For information and instructions on how to access these services, please go to www.myidcare.com/keck or call 844-801-5970 anytime between 6 am and 6 pm Pacific time, Monday through Friday excluding major holidays.

Hospital Administration
Rodney Hanners
Chief Operating Officer, Keck Medicine of USC
& Chief Executive Officer for Keck Hospitals

For More Information

For further information, please go to www.myidcare.com/keck or call 844-801-5970 anytime between 6 am and 6 pm Pacific time, Monday through Friday excluding major holidays.

We apologize for any inconvenience or concern that this notification may cause. As a member of the Trojan family, we want to ensure that we do all that we can to maintain your trust and confidence.

Sincerely,

Rod Hanners
Chief Operating Officer for Keck Medicine of USC
& Chief Executive Officer for Keck Hospitals