DATA INCIDENT NOTIFICATION

What Happened

Lakewood Health System ("LHS") was victimized by a cyber attack (the "Incident") that impacted the email account of one of our employees. We immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope, the impact on our information systems, and the identity of those the Incident affected.

On or about February 27, 2020, we determined that, on January 21, 2020, the cyber attacker may have accessed emails in the impacted account that contain personal health information ("PHI") and/or personally identifiable information ("PII"). We have not found any evidence that the information at issue was misused as a result of the Incident.

What Information Was Involved

A subset of the emails subject to the Incident contained one or multiple data elements of PHI and/or PII including names, healthcare payment information, treatment information, diagnoses, medications, medical record numbers, government identification numbers, and/or Social Security numbers.

What We Are Doing

Out of an abundance of caution, we are providing this notice so that all potentially affected individuals can take steps to minimize the risk that their information will be misused. As an added precaution, we have arranged for TransUnion to provide 12 months of free credit monitoring and related services to potentially affected individuals. To find out whether you were among those whose information was potentially affected, please contact please contact (888) 829-6561, Monday – Friday between 6am – 6pm PST; Saturday & Sunday between 8am – 5pm PST.

LHS treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. Since learning of the attack, we have taken a number of steps to further secure our systems. Specifically, we have: changed the password for the impacted account; removed the false multi-factor enrollment for the affected account, and enrolled the legitimate user in multi-factor authentication; monitored access to the impacted account; reviewed multi-factor authentication access across our network; implemented Target Threat Detection on URL's in email messages; worked with a third-party forensics expert to confirm our systems are secure; and implemented strong web security protocols.

What You Can Do

In addition to enrolling in the free credit monitoring and related services mentioned above, we recommend that you remain vigilant and take the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

    - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
    - You can also receive information from these agencies about avoiding identity theft, such as by placing a "security freeze" on your credit accounts.
    - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
    - Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
Consumer Fraud Division	Consumer Fraud Assistance	Consumer Relations & Fraud
P.O. Box 740256	P.O. Box 9556	Victim Assistance
Atlanta, GA 30374	Allen, TX 75013	1561 E. Orangethorpe Ave.
800-525-6285	888-397-3742	Fullerton, CA 92831
security.dataadministration@equifax.com	businessrecordsvictimassistance@experian.com	800-372-8391

FVAD@Transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a "security freeze" on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement, and you can also report this to the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

   Federal Trade Commission
   Consumer Response Center
   600 Pennsylvania Avenue
   NW Washington, DC 20580

For More Information

If you have questions or concerns, please contact please contact (888) 829-6561, Monday – Friday between 6am – 6pm PST; Saturday & Sunday between 8am – 5pm PST. We apologize for this situation and any inconvenience it may cause you.

4835-1233-2214, v. 1