DATA INCIDENT NOTIFICATION

What Happened

Lakewood Health System ("LHS") was victimized by a cyber attack (the "Incident") that impacted the email accounts of certain of our employees. On January 16, 2019, we determined, through our extensive investigation of the Incident, that the cyber attacker may have accessed or acquired emails in these accounts, a subset of which contain personal health information ("PHI") and/or personally identifiable information ("PII").

We commenced the foregoing investigation immediately upon learning of the Incident for the purpose of determining its scope, the impact on our information systems, and the identity of those the Incident affected. With assistance from third party experts, we determined that the cyber attack occurred between November 12 and December 18, 2018. We have not found any evidence that the information contained in the affected emails was misused as a result of the Incident.

What Information Was Involved

A subset of the emails potentially accessed or acquired by the cyber attacker contained one or multiple data elements of PHI and/or PII, including names, Social Security Numbers, driver's license numbers, dates of birth, financial account information, health information, and/or treatment information.

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 call (877) 239-1254 between the hours of 8 a.m. and 8 p.m. CT, Monday through Friday.

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: implemented Forged Email Detection and Email Spoofing Detection on our email security appliance; reset all users' network accounts; implemented mandatory network password resets every 90 days; and undergone a health check with our email security vendor. We are also implementing multi-factor authentication and will routinely test and train our users on identifying and properly responding to email phishing campaigns.

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
P.O. Box 740256	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com/consumer	www.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 call (877) 239-1254 between the hours of 8 a.m. and 8 p.m. CT, Monday through Friday. We apologize for this situation and any inconvenience it may cause you.

4825-9368-3337, v. 1