Notice of Data Security Incident

Signature Healthcare Corporation ("SHC") is committed to the privacy of individuals and takes the protection of personal information that is entrusted to us seriously. Although we have no reason to believe that patient information has been used to commit fraud or identity theft, we are making our patients aware of a recent data security incident that may have involved personal information. On November 4, 2021, we discovered that, beginning on or about October 16, 2021, someone outside of SHC temporarily accessed email accounts of clinician employees without authorization.

Upon learning of the situation, we promptly began an internal investigation and contained the incident by securing the accounts to prevent further access. We also hired a leading forensic security firm to further investigate the incident and confirm the security of our computer systems and network.

At this time, we do not believe that the unauthorized third party's motivation was to access patient personal information contained in the email account, and have no indication that any such information has been used for fraud against a patient. However, out of an abundance of caution, SHC is notifying potentially involved individuals directly via physical mail and through this notice. SHC has committed to taking steps to help prevent something like this from happening again, including reviewing its technical controls and procedures.

As part of our investigation, we reviewed the email account for personal information. While SHC is not aware of any instances of actual access to patient information, the account would have contained one or more of the following data elements for patients: patient's first and last name, sex, date of birth, dates of visits, test results, medical record number, diagnosis and medical history.

To date, there is no indication of any identity theft or fraud occurring as a result of this incident; however, as a precautionary measure, involved individuals should remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing their account statements, monitoring their credit reports closely, and notifying their financial institutions if unusual activity is detected. Individuals should also promptly report any fraudulent activity or suspected identity theft to proper law enforcement authorities, including the police and their state's attorney general. Individuals may also wish to review the tips provided by the Federal Trade Commission ("FTC") on fraud alerts, security/credit freezes and steps that they can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). Individuals may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Contact information for the three national credit reporting agencies is as follows:

Equifax	Experian	TransUnion
1-800-349-9960	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016

For further information and assistance, please call (855) 618-3183 from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding some U.S. holidays).