HIPAA Substitute Notice

Important Information Regarding Data Security Incident

Guidehouse, a global provider of professional services, recently learned in late March 2021 that it had been the victim of a cyber-attack. The attack occurred in late January 2021, and involved the compromise of a third-party service used for secure file transfer for clients including East Jefferson General Hospital and Metairie Physician Services, Inc. This incident did not involve any unauthorized access to internal systems maintained by Guidehouse. Guidehouse provides services to East Jefferson General Hospital and Metairie Physician Services, Inc. involving medical claims processing. **Three Hundred Sixty individuals who made appointments or sought medical treatment at East Jefferson General Hospital and/or Metairie Physician Services, Inc. may have been impacted.**

Upon learning of the incident, we immediately launched an investigation and have since ceased using the third-party service that had been compromised. We have cooperated with federal law enforcement and engaged leading cyber security experts in connection with investigating and responding to the incident. Based on the nature of the incident, it has taken time to accurately determine what data was impacted. After determining East Jefferson General Hospital and Metairie Physician Services, Inc. information was impacted, we notified East Jefferson General Hospital and Metairie Physician Services, Inc. on May 18, 2021.

The personal information involved in this incident may have included names and dates of birth, member IDs, addresses, and certain medical information relating to individual patients of our client East Jefferson General Hospital and Metairie Physician Services, Inc.

This incident did not involve any unauthorized access to any systems or files maintained by East Jefferson General Hospital and Metairie Physician Services, Inc. information technology systems. We are not aware of any misuse of the information.

We are not aware of any misuse of your information. Consistent with certain laws, we are providing you with the following information about steps that a consumer can take to protect against potential misuse of personal information.

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at www. ftc.gov/idtheft, or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

HIPAA Substitute Notice

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under the federal Fair Credit Reporting Act ("FCRA"), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(888) 909-8872

You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you can contact the nationwide credit reporting agencies at the phone numbers listed above to place a security freeze to restrict access to your credit report.

You will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

On July 15, 2021, we began providing notice of the incident to impacted individuals for whom we had contact information. Individuals seeking additional information regarding this incident can call (833) 541-1593. Please know that we regret any inconvenience or concern this incident may cause.