Decatur County General Hospital

January 26, 2018

Dear Patient:

Decatur County General Hospital takes the privacy and security of its patients' health information seriously. We are writing to let you know about an incident involving an electronic medical record (EMR) system used by our hospital. On November 27, 2017, we received a security incident report from our EMR system vendor indicating that unauthorized software had been installed on the server the vendor supports on our behalf. The unauthorized software was installed to generate digital currency, more commonly known as "cryptocurrency." Following receipt of the incident report, we began our own investigation into the incident. At this time, our investigation continues, but we believe an unauthorized individual remotely accessed the server where the EMR system stores patient information to install the unauthorized software. The software was installed on the system at least as of September 22, 2017, and the EMR vendor replaced the server and operating about four days later.

Over the past several months, there have been numerous news stories about computer systems around the country being affected by similar incidents involving the unauthorized installation of this type of software. Again, while our investigation continues into this matter, we have no evidence that your information was actually acquired or viewed by an unauthorized individual, and based upon reports of similar incidents, we do not believe that your health information was targeted by any unauthorized individual installing the software on the server. Our investigation to date, however, has been unable to reasonably verify that there was not unauthorized access of your information. Information contained on the affected server included demographic information such as patient names, addresses, dates of birth, and Social Security numbers, clinical information such as diagnosis and treatment information, and other information such as insurance billing information.

Complimentary Credit Monitoring Service

As a safeguard, we have arranged for online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies, at no cost to affected patients. If you have been a patient at Decatur County General Hospital, please call 1-877-760-4702 to see if you are eligible.

Directions for Placing a Fraud Alert

Additionally, you may choose to adopt an increased level of protection by placing a fraud alert on your credit file at the three major credit bureaus. A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. An initial fraud alert lasts 90 days. You may also place a security freeze, or credit freeze, on your credit file which is designed to prevent credit, loans, and services from being provided in your name without consent. However, setting a security freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. Contact information for the three major bureaus is provided below:

Equifax (equifax.com)	Experian (experian.com)	TransUnion (transunion.com)
1-888-766-0008	1-888-397-3742	1-888-909-8872
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016

As a general matter, you should remain vigilant by regularly reviewing financial account, medical bills and health insurance statements, such as explanations of benefits (EOB). The Federal Trade Commission (FTC) recommends that you check your credit reports periodically to help spot problems. You can obtain a free credit report annually from each of the three major credit bureaus by calling 1-877-322-8228 or by visiting www.AnnualCreditReport.com. You should promptly report any suspicious activity or suspected identity theft to us

and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the FTC. For more information about identity theft and other forms of financial fraud, as well as information about fraud alerts and security freezes, you can contact the FTC online at www.ftc.gov/idtheft, by mail at Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, or by calling 1-877-ID-THEFT (438-4338). Regularly monitoring financial and other account activity and periodically obtaining and reviewing credit reports are prudent steps to take given the prevalence of identity theft and related crimes.

Again, our investigation into this incident continues but we do not believe the motivation of any unauthorized access to the EMR server was to access or acquire your information. We encourage you, however, to exercise caution regarding communications if you receive an unsolicited call or email about this incident. Please know that we will not call or email anyone requesting any personal information as a result of this situation.

We take protecting our patients' information seriously, and we regret any inconvenience or concern this unfortunate incident has caused you. Decatur County General Hospital has set up a dedicated number for you to call with any questions or for more information. Should you have any questions, please do not hesitate to call 1-877-760-4702, Monday through Friday (except holidays), 8:00 am to 8:00 pm Central Time.

Sincerely,

Decatur County General Hospital