Notice to Our Patients About the December 2018 Email Phishing Incident

Memorial Hospital at Gulfport (“MHG”) values the privacy and confidentiality of our patients’ information. This notice is an update regarding our December 2018 email phishing incident.

On December 17, 2018, we learned that an unauthorized third party gained access to an employee’s email account on December 6, 2018. We immediately took steps to secure the account and began an investigation. Our investigation determined that patient information was contained in the email account and may have included patients’ names, dates of birth, health insurance information, Social Security numbers and/or information about medical care received at MHG. A limited number of financial account and payment card numbers were also included in the email account.

We initially notified patients and the public of this incident on February 15, 2019, and continued our investigation. Our ongoing investigation has revealed additional patients and patient information contained in the email account. Beginning on June 14, we are sending additional letters to patients who have been identified during the course of our investigation.

While we have no indication that patient information has been misused in any way, we are offering complimentary credit monitoring and identity protection services to those patients whose Social Security numbers may have been affected. We also recommend that affected patients carefully review statements they receive from their banking institutions, payment card issuers, health care providers and health insurers. If they see charges or services not incurred or received, they should contact the issuing bank, provider or insurer, as applicable, immediately.

If patients have any questions about this incident, please call 1-855-579-3699, Monday through Friday, 8 a.m. to 5:30 p.m. Central Time.

We deeply regret any concern or inconvenience this may cause our patients. MHG takes the privacy and confidentiality of our patients' information very seriously and is enhancing information security safeguards to help prevent an incident such as this from occurring in the future.