Monroe Surgical Hospital patient data may have been compromised in a cyber breach of IBERIABANK's vendor, Technology Management Resources, Inc.

What happened?

Monroe Surgical Hospital uses an IBERIABANK lockbox service, which collects and processes payments from our patients and customers. In turn, IBERIABANK uses a third party, Technology Management Resources, Inc. (TMR), to scan and process the payments and other pertinent payment data received in the lockbox. Monroe Surgical Hospital has no relationship with TMR.

On July 2, 2020, TMR discovered that a TMR employee's user account had been compromised. Monroe Surgical Hospital received formal notice of this incident on October 13, 2020 and has since been actively seeking information regarding this incident.

TMR reported that when they discovered the incident, they immediately secured the account and began an investigation in consultation with external cybersecurity professionals. TMR has stated that their investigation determined that the cybercriminal, or threat actor, may have viewed images of checks and related images containing potential Protected Health information (PHI) related to patients of Monroe Surgical Hospital. According to TMR, the threat actor activity occurred between August 5, 2018 and May 31, 2020, with the bulk of activity occurring between February and May 2020. TMR notified the FBI of this incident. This incident is believed to be part of a wider effort by an unknown cybercriminal to attack TMR customers beyond IBERIABANK.

What information was involved? According to TMR, the investigation concluded that the threat actor potentially viewed images containing PHI within TMR's application. The PHI on these images may have included certain patients' names, addresses, dates of birth, patient and health insurance account numbers, procedure type, provider name and treatment cost information.

How will I know if my information was exposed? If your information was a part of this incident, you will receive a letter in the mail from IBERIABANK in the coming days.

What is the Monroe Surgical doing in response? Monroe Surgical Hospital takes the privacy and security of our patients' information very seriously. Fortunately, the hospital and its internal security and computer systems were not involved in this breach. IBERIABANK, however, is offering our affected patients and customers credit monitoring and identify theft protection through CyberScout in order to give peace of mind. Information regarding these services will be provided in the letter from IBERIABANK.

What has TMR done to prevent future incidents? TMR reports that it has taken several corrective actions to remediate the security incident, prevent a further security incident, and mitigate the effects of this security incident. According to TMR, its credentials have been reset or deactivated (as applicable). TMR also reports that it implemented additional rules in its firewall to more tightly control the ability to access its application from other countries, among other steps taken.

What can you do? As a best practice, we encourage our patients and customers to remain vigilant against incidents of identity theft and fraud. Review your financial account statements and claims

information from your health insurance provider and monitor credit reports for suspicious activity. If you find any suspected issues related to this incident you should notify the proper law enforcement authorities and report them to IBERIABANK by calling toll-free 1-888-905-0513 Monday through Friday, 8 a.m. to 8 p.m.

You can also use this number if you do not receive a letter from IBERIABANK but are still concerned that your information was potentially affected by this incident.

We apologize for any inconvenience that may have been caused by this TMR security incident. If you have additional questions, you can call our toll-free number at 855-258-3746 or email us at privacy@monroesurgical.com.