Southwest Washington
Regional Surgery Center

Notice Regarding Data Security Incident

Southwest Washington Regional Surgery Center, LLC ("SWRSC") is committed to maintaining the privacy and security of patient information. On November 6, 2018, SWRSC notified 2,393 patients about a security incident involving an email phishing attack, which affected one employee's email box between May 27, 2018 and August 13, 2018. Upon learning of the situation, SWRSC promptly launched an investigation and engaged external cybersecurity professionals.

After an extensive forensic investigation and manual email review, SWRSC discovered on September 25, 2018 that the impacted email account that was accessed contained some Protected Health Information, including some patients' names, Social Security numbers, driver's license numbers, and/or medical information (diagnosis, treatment, surgery, medications, labs and/or health insurance information). A limited number of patients' credit card numbers were also contained in the impacted email account. This incident does not affect all SWRSC patients.

SWRSC has no evidence that any of the information has been misused. The patients whose Social Security numbers and/or driver's license numbers were contained in the impacted email account may enroll in a credit monitoring and identity theft restoration service, which is being offered at no cost. Patients have also been provided with best practices to protect their information, including steps to obtain a free credit report, placing a fraud alert and/or placing a security freeze on their credit files. Patients have been reminded to remain vigilant in reviewing financial account statements on a regular basis for any fraudulent activity. It is also recommended that affected patients review the explanation of benefit statements that they receive from their health insurance providers and follow up on any items not recognized.

SWRSC has taken steps to minimize the risk of a similar incident in the future, including updating passwords and enhancing email access protocols.

For further questions or additional information regarding this incident, or to determine if you may be impacted by this incident, a dedicated toll-free response line has been set up at 888-891-8399. The response line is available Monday through Friday, 6 a.m. to 6 p.m. Pacific Time.

###