A Notice to Our Patients

Atrium Health Wake Forest Baptist is committed to protecting the confidentiality and security of our patients' information. Regrettably, we recently identified a security incident that may have involved some of that information.

On April 20, 2023, we learned that an unauthorized third party gained access to an employee's email account on that same day through phishing. "Phishing" occurs when an email is sent that looks like it is from a trustworthy source, but it is not. The malicious email misleads the recipient to share or provide access to their account login information.

We immediately began an investigation, took the necessary steps to secure the affected account and confirmed the unauthorized third party had no further access. We also engaged a computer forensic firm to assist us with our investigation and notified law enforcement. Based on our findings, it appears the unauthorized third party had access to the affected account for a short time between April 18, 2023 – April 20, 2023. The forensic examination indicated the activity of the unauthorized third party was not focused on email content pertaining to medical or health information.

Unfortunately, it was not possible to conclusively determine whether the unauthorized third party actually viewed any emails or attachments in the account. As a result, we conducted a review of the account to determine what information may have been accessible to the unauthorized third party. The information involved varied by individual, but generally included names, dates of birth, hospital account record numbers, health insurance information, treatment cost information, and/or clinical information, such as dates of service, provider names or locations of service. In some instances, patients Social Security numbers were also identified in the account.

Not all of Wake Forest Baptist's patients were impacted, only those whose information happened to be in the files used by the employee's account. Additionally, our electronic medical record systems are separate from our email accounts and were **not** affected by this incident.

We have no indication that anyone's information was actually viewed by the unauthorized third party or that it has been misused. However, as a precaution, we are mailing notification letters to individuals whose information was identified through our review and for whom we have sufficient contact information. The notification letters include a Reference Guide that provides additional information on general steps individuals can take to monitor and protect their personal information. Although we are unaware of any actual or attempted misuse of patient information as a result of this incident, we encourage affected patients to carefully review their credit reports and similar types of documents that might indicate questionable activity. For those whose Social Security numbers were identified in the account, we are offering complimentary credit monitoring and identity protection services.

We have also established a dedicated, toll-free call center to answer questions that individuals may have about the incident. If you have questions, please call 866-547-5833, available Monday through Friday, from 9 a.m. to 6:30 p.m. Eastern Time, excluding major holidays.

We apologize for any concern or inconvenience this incident may have caused and remain committed to protecting the confidentiality and security of our patients' information. We have and will continue to enhance our security controls, as appropriate, to minimize the risk of similar incidents in the future. We also continue to provide phishing training and education to our employees.