Notice to our Patients of Lab Privacy Incident

Sentara Health values and respects the privacy of our patients' information. Regrettably, this notice concerns an issue that may have involved some of that information.

In December, the Sentara Health's Lab Services department hired an individual to process lab requisitions. Lab requisitions are the orders a provider sends to a lab to tell them what type of lab tests to run on a patient.

The individual was hired to work remotely, meaning he did not work in an office located on Sentara property. In January, after a virtual meeting with the individual, the individual's manager made Sentara's Privacy Department aware of concerns related to the individual's identity, including whether the individual with whom the manager had been interacting was the person initially hired. In response to the manager's report, the individual's access to Sentara's systems was immediately terminated. We subsequently learned that the individual's activity is consistent with a job-sharing scam. In this type of situation, an individual may seek employment from multiple employers while farming the work out to other individuals who receive a percentage of the pay. This enables a person to be hired by a company as an employee and share the job duties with other people without the employer's knowledge.

Sentara promptly initiated an investigation into this concern with the assistance of a third-party forensic firm and notified federal law enforcement. On or about January 28, 2025, the investigation determined that the individual's access to data stored within Sentara's electronic medical records system appeared consistent with job-related activities. However, because we were unable to confirm whether the access was by the individual hired, or by another person unauthorized to share job responsibilities, we are notifying you of this incident.

This incident did not affect all patients, but only certain patients who received lab tests between January 14 and January 23, 2025. The information the individual(s) accessed varied by patient, but may have included patient names, addresses, dates of birth, patient identification numbers, medical record numbers, telephone numbers, Social Security Numbers, the lab tests that were ordered, the name of the provider who ordered the tests and the date the labs were ordered.

We want our patients to know that we are taking this matter very seriously. We began mailing letters to affected patients on March 28, 2025, and are offering patients complimentary credit monitoring and identity protection services. Information on how to activate those services is included in the letters being sent to those patients. We have also established a dedicated call center to answer any questions patients may have. If you believe you are affected and do not receive a letter by April 25, 2025, please call 1-800-511-4722, Monday through Friday, 9 a.m. to 6:30 p.m. Eastern Time.

We take our responsibility to safeguard personal information seriously and apologize for any concern this incident might cause. We are committed to taking steps to help prevent something like this from happening again, including evaluating additional platforms for educating staff and reviewing technical controls.