A Notice to Our Patients

Erlanger Health System is committed to protecting the confidentiality and security of our patients' information. Regrettably, this notice concerns a security incident by a third-party vendor that may have involved some of that information.

On June 12, 2020, an employee of a third-party vendor at Erlanger misplaced backups CDs used to perform software updates, which contained patient information. Upon being notified of the missing CDs by the third-party vendor, we performed an investigation and an extensive search of the relevant area of the Hospital; however, the CDs were not found. On July 7, it was determined that the CDs were not password-protected as previously reported.

This incident did not affect all Erlanger patients, only those patients whose information was contained on the missing CDs. The data stored on the CDs contained information about certain patients' care, including names, dates of birth, medical record or patient account numbers, service dates, and lab results. The following information was not stored on the CDs: contact information, Social Security numbers, credit card information, insurance information, or other financial-related data.

As a precaution, we are mailing letters to patients whose information was stored on the CDs. We have also established a dedicated, toll-free call center to answer patients' questions. If you have questions, please call 1-877-476-4111, Monday through Friday, from 8 a.m. to 5 p.m. Eastern Time. We recommend that affected patients review any statements they receive from their healthcare providers. If patients see services they did not receive, they should contact the provider immediately.

We are committed to protecting the privacy of our patients' information and continuously work toward improving our processes and systems. We deeply regret any concern or inconvenience this incident by a third-party vendor may cause you. As a result of this incident, we are working with the third-party vendor to eliminate the use of CDs when performing backup services and are requiring that all backup information be stored in a secure location on the Hospital's network. We are also providing additional education to re-enforce the importance of safeguarding equipment that may contain patient information.