Notice to Our Patients of a Data Security Incident

Lawrence General Hospital ("LGH") is committed to protecting the confidentiality and security of our patients' information. This notice informs our community about a data security incident that may have involved a limited subset of patient information.

On September 19, 2020, we identified a data security incident that disrupted the operations of our IT systems. We immediately took steps to secure our systems, notified law enforcement, and launched an investigation. LGH's investigation determined that an unauthorized party may have accessed its IT systems between September 9, 2020 and September 19, 2020. During this time, the unauthorized party may have accessed a limited subset of patient information. This information may have included names, LGH-assigned patient identification numbers, insurance type, and LGH-assigned visit identification numbers. In some very limited instances, clinical information may have been subject to unauthorized access. Fewer than 5 individuals had their Social Security numbers potentially involved.

The investigation confirmed that this incident did **NOT** involve unauthorized access to any employee information, such as Social Security numbers or financial account information.

On November 5, 2020, we began the process of mailing notification letters to individuals whose information may have been involved in the incident. In addition to mailing letters, we have established a dedicated, toll-free call center to answer questions that patients may have. If you have questions, please call 833-256-3153, Monday through Friday, between 9:00 a.m. and 11:00 p.m., and Saturday and Sunday, between 11:00 a.m. and 8:00 p.m., Eastern Time.

We recommend that patients whose information may have been involved in this incident review the statements they receive from their health care providers. If they see services they did not receive, patients should contact the provider immediately.

We deeply regret any concern or inconvenience this incident may cause our patients. To help prevent something like this from happening again, we have implemented enhanced, continuous monitoring and alerting software on our IT systems.