Emory Healthcare’s Orthopaedics & Spine Center and Brain Health Center within Emory Clinic used an application called Waits & Delays to update patients regarding their appointments. This database contained limited information used in updating appointment information including patients’ names, dates of birth, contact information, internal medical record numbers, and basic appointment information such as dates of service, physician names and whether patients required imaging (but not the type of imaging). The database did not contain patients’ Social Security numbers, financial information, diagnosis or other electronic medical record information.

On January 3, 2017, we learned that there was unauthorized access to the Waits & Delays database around the New Year’s weekend after someone deleted the database and demanded that EHC pay to have it restored. We learned that there was another unauthorized access by an independent security research center that searches out vulnerabilities in applications and traditionally notifies the company so that it can be remedied.

Once EHC learned that this third-party database was accessed improperly, we immediately initiated an internal investigation, alerted law enforcement and are in the process of notifying impacted patients. Additionally, we are taking this opportunity to further review and refine our security measures relating to internal and third-party computer systems.

It is important to note that EHC does not have any indication that any patient information has been used inappropriately.

The incident did not impact all patients of EHC, but affected only patients who either:

1. Had an appointment at the Orthopaedics & Spine Center within Emory Clinic between March 25, 2015 and January 3, 2017; or
2. Had an appointment at the Emory Clinic Brain Health Center between December 6, 2016 and January 3, 2017.

If you have been impacted, you will receive a notice in the mail with additional information. Patients who did not have an appointment with these Centers and within the dates listed above were not impacted.
Please refer to the notice you will receive in the mail regarding steps that you can take to protect yourself. In general, we recommend, as a precautionary measure, that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state’s attorney general.

If you have any additional questions, you may call our confidential inquiry line at 844-856-9325 toll-free, between 9:00 a.m. and 9:00 p.m., Eastern Time, Monday through Friday.