UMassMemorial
Community Healthlink

A Notice to our Patients

UMass Memorial Community Healthlink ("CHL") takes the privacy and security of its patients' information very seriously. Regrettably, this notice concerns an incident involving some of that information.

On April 18, 2019, we learned that an unauthorized individual gained access to two CHL employees' email accounts. The access was for a limited time on April 18th. We immediately secured the accounts, began an investigation, and a leading computer forensic firm was engaged to assist. The investigation was unable to determine whether the unauthorized person actually viewed any emails in the account. As a result, we reviewed all emails in the accounts to identify patients whose information was contained in an email or attachment in the accounts and therefore may have been accessible to the unauthorized person. During this review, we determined that the accounts contained some of our patients' information, including patients' names, dates of birth, client identification numbers, diagnosis and treatment information, health insurance information, and in limited instances, Social Security numbers.

This incident did not affect all CHL patients, only those patients who had information contained in the affected email accounts.

We have no indication that any patient information was actually viewed or misused. However, we have begun mailing letters to patients whose information was identified in the accounts. We have also established a dedicated call center to answer questions for affected patients. If you have questions about this incident, please call 1-877-420-0507, from 8:00 a.m. to 5:00 p.m. Eastern time, Monday through Friday. The letters provide additional information about how affected patients can protect themselves. For those patients whose Social Security number was contained in the email accounts, we are offering complimentary credit monitoring and identity protection services. We also recommend affected patients review any billing or explanation of benefits statements they receive from their health insurers or healthcare providers. If they see services they did not receive, they should contact the health insurer or provider immediately.

We regret any concern or inconvenience this incident may cause. We remain committed to protecting the confidentiality and security of our patients' information. To help prevent something like this from happening in the future, we forced a password change for the impacted employees' accounts, strengthened rules to block additional outside domains and impersonation attempts, increased automated alerts, and have implemented additional measures to further strengthen our security processes. We are also reinforcing employee training on how to detect and avoid phishing emails.