Website Notice

Health Quest is committed to protecting the confidentiality and security of our patients' and employees' information. Regrettably, this notice concerns an incident involving some of that information.

On October 25, 2019, through our investigation of a phishing incident, we determined some patient information may have been contained in an email account, accessed by an unauthorized party. We first learned of a potential incident in July 2018, when numerous Health Quest employees were deceived by a phishing scheme. This resulted in certain Health Quest employees being tricked into inadvertently disclosing their email account credentials to an unauthorized party. The employee email accounts in question were secured and a leading cybersecurity firm was engaged to assist us in our investigation. As part of the investigation, we performed a comprehensive review of the voluminous contents of the email accounts in question to determine if they contained any sensitive information. HQ mailed some notification letters in May, 2019. Upon further investigation, HQ determined additional notices were required.

We determined emails and attachments in some employees' email accounts contained information pertaining to current and former patients and employees. The information involved varied by individual, but may include names in combination with, dates of birth, Social Security numbers, Medicare Health Insurance Claim Numbers (HICNs), driver's license numbers, provider name(s), dates of treatment, treatment and diagnosis information, health insurance plan member and group numbers, health insurance claims information, financial account information with PIN/security code, and payment card information.

We have no indication any patient information was viewed by the unauthorized person or has been misused. However, out of an abundance of caution, we began mailing letters to affected patients on January 10, 2020, and have established a dedicated call center to answer questions patients may have. If you have any questions regarding this incident, please call 1-844-967-1236, Monday through Friday, between 9 a.m. and 6:30 p.m. EST.

We deeply regret any inconvenience or concern this incident may cause you. We continually evaluate and modify our practices to enhance the security and privacy of our patients' and employees' information. To help prevent something like this from happening in the future, we have implemented multi-factor authentication for email and additional procedures to further expand and strengthen security processes. We are also providing additional training to HQ employees regarding phishing emails and other cybersecurity issues.