Notice of Data Security Incident

Mercy Iowa City ("Mercy") recently discovered an incident that may have involved the personal information or protected health information of some of its patients. Although Mercy has no reason to believe that any personal information or protected health information has been misused for the purpose of committing fraud or identity theft, or that any personal information or protected health information was actually viewed by any unauthorized party, it is notifying the potentially impacted patients to advise them about the steps it has taken to address the incident and provide them with guidance on what they can do to protect themselves.

Mercy discovered that an unauthorized person gained access to the email account of one Mercy employee from May 15, 2020 until June 24, 2020. Upon learning of the incident, Mercy immediately took action to secure the employee's email account to prevent any further access. Mercy also launched an investigation and engaged a leading forensic security firm to assist in its investigation. As part of that investigation, Mercy searched the account for any personal information or protected health information. Mercy completed its investigation and determined on October 3, 2020 that the account contained personal or protected health information for certain individuals. That information included, depending on the affected individual, their name, date of birth, Social Security number, driver's license number, medical treatment information, and medical insurance information.

On November 13, 2020, Mercy began sending written notifications to individuals whose personal information or protected health information was contained in the email account for whom it has contact information, and arranged for complimentary identity theft protection services for those individuals whose Social Security numbers and/or driver's license numbers were involved in the incident.

Affected individuals should refer to the notice they will receive in the mail regarding steps they can take to protect themselves. Again, Mercy has no reason to believe that any personal information has been misused for the purpose of committing fraud or identity theft, but as a precautionary measure, impacted individuals should remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing their account statements and monitoring credit reports closely. If individuals detect any suspicious activity on an account, they should promptly notify the financial institution or company with which the account is maintained. They should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and their state's attorney general.

Affected individuals may also wish to review the tips provided by the Federal Trade Commission ("FTC") on fraud alerts, security/credit freezes and steps that they can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). Affected individuals may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Mercy deeply regrets any concern or inconvenience this incident may cause its clients. Mercy is reinforcing information security procedures with its employees and implementing changes to help prevent an incident like this from happening again. Additional information is available via a confidential, toll-free inquiry line at 855-914-4658 from 8:00 a.m. to 8:00 p.m. Central, Monday through Friday.