

Notice of a Data Incident

Cookeville Regional Medical Center (“CRMC”) discovered a data incident that involved the personal information of certain individuals. On July 14, 2025, CRMC discovered suspicious activity in its computer network. Upon discovering the incident, CRMC promptly began an internal investigation, worked to secure its systems, and notified law enforcement. CRMC also engaged a forensic security firm to assist with its investigation and ensure the security of its computer network. The forensic investigation determined that an unauthorized third party accessed CRMC’s computer network and viewed or acquired certain files between July 11, 2025, and July 14, 2025.

Based on the results of its investigation, CRMC conducted a comprehensive review of the affected files to determine if they contained any personal information that was viewed or acquired by the third party. CRMC identified the personal information of certain individuals. Depending on the individual, the personal information may include their name, address, date of birth, Social Security number, driver’s license number, financial account number, medical treatment information, medical record number, and/or health insurance policy information. CRMC is mailing notification letters to individuals for whom they have a valid address and whose information was in the affected files.

Notified individuals should refer to the notice they will receive in the mail for the steps they can take to protect themselves. Although CRMC has no evidence that any information may have been misused as a result of this incident, as described in those letters, CRMC has 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. As a precautionary measure, individuals should remain vigilant about protecting themselves against potential fraud and/or identity theft including by 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 the company that maintains the account. 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. Notified 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). Notified individuals may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Contact information for the three national credit reporting agencies is as follows:

P.O. Box 105788
Atlanta, GA 30348

Experian
[1-888-397-3742](tel:1-888-397-3742)
www.experian.com

P.O. Box 9554
Allen, TX 75013

TransUnion
[1-800-888-4213](tel:1-800-888-4213)
www.transunion.com

P.O. Box 1000
Chester, PA 19016

CRMC is committed to maintaining the privacy and security of the information entrusted to it. CRMC has taken, and is taking, additional steps to help reduce the likelihood of a similar event from happening in the future, including by enhancing its technical security measures. Individuals seeking additional information may call a confidential, toll-free inquiry line at 877-396-3267 from 8:00 a.m. – 8:00 p.m. Central Time, Monday through Friday.

QUICK LINKS