TN Division of TennCare

February 2024

HealthEC Data Breach Information

Recently, HealthEC LLC (HEC), a population health technology company that provides services to entities nationwide, including TennCare, experienced a data breach and, as required, provided or will provide notice to potentially impacted TennCare members and providers. Because of the scope of the breach, you may have or receive questions or comments about this incident. The FAQs below provide additional information.

What Happened?

HEC, which works with TennCare and partner providers to better coordinate care for members, became aware of suspicious activity potentially involving its network and customers nationwide and promptly began an investigation. The investigation determined that certain systems were accessed by an unknown actor between July 14, 2023, and July 23, 2023, and during this time certain files were copied and held for ransom by the unknown actor. Once learning of the suspicious activity from HEC, TennCare immediately suspended operation of the Care Coordination Tool (CCT) and all other HEC functions.

Working with the Federal Bureau of Investigation and the Department of Homeland Security, HEC engaged a third-party vendor and undertook a thorough review of the systems and files in order to identify what specific information was present in affected files and to whom it relates. This review was completed in late October and confirmed a data breach of information relating to HEC's clients, including TennCare.

Once TennCare received confirmation of the breach from HEC, TennCare worked with HEC to identify and notify potentially impacted individuals. Notification to individuals identified as potentially impacted began around December 22.

Additionally, address verification for some potentially impacted individuals was completed later and, therefore, those individuals continue to receive notifications.

Who is impacted by the breach?

We have no confirmed evidence of any specific TennCare member's or provider's individual information being compromised or disclosed. However, because information related to TennCare members and providers was potentially vulnerable, all potentially affected TennCare members and providers are being mailed notifications.

What data is included?

The types of information identified through HEC's review varies by individual but may include name, address, date of birth, Social Security number, Taxpayer Identification number, medical record number, medical information, and/or billing and claims information.

What is being done to mitigate any negative impact on a TennCare member or provider?

Impacted individuals are entitled to 12 months of credit monitoring and identity protection from the date of enrollment paid for by HEC. Information relative to enrollment in these services and other protection measures available for affected individuals has been provided in the notification letter. Individuals may also call the dedicated assistance line set up by HEC at 1-833-466-9216 for help with enrollment. TennCare has also worked with the HEC to extend the timeframe for enrollment beyond 90 days from the date of the notification letter.

Why was it necessary for TennCare to share data with HEC?

As part of its scope of work, HEC provided population health services to TennCare. Functions in the requirements include operation of the CCT as well as capabilities to perform member care management functions; coordination of member care among providers; reporting on member and provider healthcare information; and reports and dashboards to TennCare and providers to manage their members. These functions require TennCare to share with HEC comprehensive information about members and providers in order to allow appropriate identification, attribution and matching, care and quality monitoring and improvement activities.

What vetting process does TennCare do to ensure proper security measures are in place for contract partners?

TennCare undertakes a number of steps to review and monitor the privacy and security protocols of partners and vendors, including:

- Implementation of strict contractual requirements with respect to system and data security, including operational and technical controls. Examples include file encryption, system firewalls, workforce training, role-based access policies, and secure and timely data deletion elements.
- Submission and review of system security plans and privacy impact analyses.
- Requirements for independent third-party security assessments of system controls and design.
- Review of system architecture by a technical review team.

What consequences will HEC face?

TennCare has notified and provided information to the Tennessee Attorney General's Office as well as other necessary federal agencies. In addition, TennCare is currently taking the necessary steps to terminate the business relationship with HEC and damages related to the incident will be assessed.

What is TennCare doing to mitigate the possibility of future data breaches and impact?

While no organization or entity can guarantee the complete prevention of data breaches, TennCare data governance efforts and technology improvements continue to improve the quality, availability and use of our data while ensuring compliance with privacy and security regulations.

TennCare regularly monitors its privacy and security requirements for partners and vendors to ensure those entities are held to the strictest possible standards in protecting member and provider information. To support this effort, TennCare has in recent years created multiple governance review teams related to data and security.

Moreover, TennCare is the middle of a significant multi-year IT transformation and modernization effort to improve the performance, reliability, and security of the services provided to TennCare members, providers and partners. In part, this effort will ensure the privacy and security of its data while improving its availability and use. Specific advancements include the implementation of the Integrated Services Layer and the Data Ecosystem, which are well underway. These improvements will allow TennCare to take advantage of the latest technology in web service transport channels, data exchange, and content management. Combined with stricter data standards, consistent data quality requirements, and improved data use capabilities, TennCare will be able to deliver secure, targeted data faster to our partners, vendors, and providers.

What if I do not receive a letter?

You may not be impacted. However, if you would like to confirm if you are impacted, you can contact the dedicated assistance line at 1-833-466-9216.

What if my organization receives letters for members and/or individual providers?

Letters to individuals were mailed to the last known address of record after attempted verification through the National Change of Address database. You may receive letters that are for patients, TennCare members, individual providers, or former providers if your organization was the last known address of record.

Organizations are not responsible for notifying individuals of this breach and both TennCare and HEC are using multiple channels to provide notice and information to the public. Organizations can collect and send letters that were mistakenly received on behalf of individuals to TennCare. You can send them to:

Division of TennCare
Attn: Privacy Office
310 Great Circle Road
Nashville, TN 37228

What should TennCare members or providers do if they have additional questions?

A dedicated assistance line has been set up by HEC at 1-833-466-9216 to help with any questions or concerns. TennCare has also set up a website with information here: https://www.tn.gov/tenncare/legal/privacy-update.html. Individuals with additional questions for TennCare may contact us at privacy.tenncare@tn.gov.

To order a free credit report or request a fraud alert be placed on a credit file, individuals can visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below.

Equifax

https://www.equifax.com/personal/credit-report-services/
1-888-298-0045
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788

Experian

https://www.experian.com/help/
1-888-397-3742
Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013
Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013

TransUnion

https://www.transunion.com/credit-help

1-800-916-8800
TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094