NOTICE OF CYBERSECURITY INCIDENT

Last Updated on August 4, 2026

Well Child, Inc. was the victim of a cybersecurity incident that involved certain electronic health information of Tennessee school-aged students

What Happened

On June 1, 2026, our organization learned of a cybersecurity incident on our computer network. We activated our incident response procedures. As an immediate precautionary measure, all affected servers were taken offline. We also engaged cybersecurity professionals and began a comprehensive investigation to determine the scope of the incident
and implement additional safeguards. On June 5, 2026, we determined that certain files were taken from our temporary file storage server that could contain sensitive personal information. As a result, Well Child is undertaking a comprehensive review to determine what information was involved and to whom the information belongs.

What Information Was Involved

Based on our investigation to date, we determined that certain Vision Screening Report Files, Vision Screening Data Files, Available Students Lists, and PEDS (Parents' Evaluation of Developmental Status) assessment documents were stored on our server at the time

of the incident. The information contained in these files varied by individual and may have included protected health information ("PHI"), such as the individual's name in combination with one or more of the following: date of birth, medical record number, provider name, diagnosis, assessment or testing results, treatment date, and billing or procedure codes. In addition, for a limited number of individuals, the information may have included a Social Security number.

At this time, our investigation has not identified any evidence that the information involved has been accessed or misused for the purpose of identity theft or fraud. However, out of an abundance of caution, we are providing this notice so that affected individuals are aware of the incident and can take appropriate steps to protect their information, if they choose to do
so.

What We Are Doing

Upon learning of the incident, Well Child has worked diligently with our cybersecurity team and has followed all applicable security protocols and guidance established by the State of Tennessee. We reported the incident to federal law enforcement. We have conducted extensive reviews of our systems, strengthened our security controls, reviewed our internal security policies and protocols, and will continue to monitor our environment to prevent future incidents.

What You Can Do

As a general matter, it is best practice to remain vigilant for incidents of

identity theft and fraud, from any source, by reviewing and monitoring your family's account statements, credit reports, and explanation of benefits (EOBs) for suspicious activity and errors. If you discover any suspicious or unusual activity on your accounts, promptly contact your financial institution or the service provider.

For More Information

If you have any questions or concerns, please contact our assistance line at (901) 728-5858, Monday through Friday, 9:00 a.m. – 6:30 p.m. Eastern Time, excluding major U.S. holidays.