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.

Additional Resources and Steps Potentially Impacted Individuals May Take on Behalf of their Minor Child

Typically, a minor child under the age of eighteen (18) does not have credit in his or her name, and the consumer reporting agencies do not have a credit file in a minor child's name. To find out if your minor child has a credit report or to request a manual search for your minor child's Social Security number each credit bureau has its own process. To learn more about these processes or request these services, you may contact the credit bureaus by phone, in writing, or by visiting the below websites:

- Equifax – 1-888-298-0045; www.equifax.com
- Experian – 1-888-397-3742; www.experian.com
- TransUnion – 1-800-680-7289; www.transunion.com

To confirm the existence of a credit report in your minor child's name, or utilize any of the below-mentioned resources, you may be required to provide the following:
- A copy of the child's birth certificate;
- A copy of the child's Social Security card or a document from the Social Security Administration showing the child's Social Security number;
- A copy of your driver's license or government-issued identification, with current address;
- If you are not the child's parent, a copy of a document gives you legal authority to act on the child's behalf, such as a foster care certification or proof of legal guardianship.

Fraud Alert
You may place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert,

Please contact any of the three credit reporting bureaus listed below:

Equifax: P.O. Box 105069, Atlanta,
GA 30348-5069, 1-800-525- 6285; https://www.equifax.com/credit-fraud-alerts/

Experian:
P.O. Box 9554, Allen, TX 75013, 1-888-397- 3742; https://www.experian.com/help/fraud-alert/

TransUnion:
P.O. Box 2000, Chester, PA 19016, 1-800-680- 7289; https://www.transunion.com/fraud-alerts

Security Freeze
As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent.

However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should contact any of the three credit reporting bureaus listed below:

Equifax:
P.O. Box 105788, Atlanta, GA 30348-5788, 1-888-378-4329;
https://www.equifax.com/personal/help/place-lift-remove-security-freeze/

Experian:
P.O. Box 9554, Allen, TX 75013, 1-888-397-
3742; www.experian.com/freeze/center.html

TransUnion:
P.O. Box 160, Woodlyn, PA 19094, 1-800-916-
8800; www.transunion.com/credit-freeze

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the Federal Trade Commission (FTC). The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. You have the right to file a police report on behalf of your minor child if they ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that your minor child has been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.