

NOTICE OF DATA INCIDENT

What Happened?

On March 3, 2025, the Counseling Center for Wayne & Holmes Counties (the “Counseling Center” or “we”) was alerted to suspicious activity by our third-party service provider after experiencing a disruption in our systems. Our priority is the care and well-being of the individuals we serve. Upon learning this, we immediately began an internal investigation, and started taking steps to identify, contain, and address any unauthorized activity. We isolated any systems we believe were impacted, reset account credentials, and engaged leading data security and privacy professionals to assist in a thorough forensic investigation.

The forensic investigation determined that an unauthorized entity likely gained access to one (1) of the Counseling Center’s servers on March 2, 2025, and took information from our systems on March 3, 2025. Due to the swift response of our team, we were able to contain the incident and minimize any further unauthorized activity. There is no evidence that any individual’s personal information has been used for identity theft or fraud.

What Information Was Involved?

Based on the findings of the investigation, the following types of information may have been impacted: name, date of birth, Social Security number, driver’s license or state identification number, health insurance information, medical condition information, treatment provider name, medical record number, treatment cost information, and diagnosis and/or treatment information. Note that this describes general categories of information identified as present within the affected Counseling Center system during the incident and includes categories that are not relevant to each individual whose information may have been present.

What We Are Doing.

We take this incident and the safety of the individuals we serve very seriously. Upon becoming aware of the incident, we took immediate action to contain the situation and worked closely with data security and privacy professionals to further strengthen our existing, significant safeguards. After determining unauthorized activity occurred, we began a thorough analysis of the information involved to identify those potentially affected and notify them. This data analysis concluded on December 9, 2025, and we have worked continuously to notify affected individuals and appropriate regulatory authorities.

What Can Impacted Individuals Do?

We encourage individuals to remain attentive against potential identity theft and fraud, regularly monitor free credit reports, review account statements, and report any suspicious activity to financial institutions. Under U.S. law, individuals are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus. Presented below are steps that individuals can take to protect their personal information, including health and medical information.

Steps You Can Take to Protect Your Personal Information

To obtain a free credit report, individuals may visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228.

Alternatively, affected individuals can contact the three (3) major credit reporting bureaus directly at the addresses below:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, <https://www.transunion.com/data-breach-help>, 1-833-799-5355

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft pursuant to the Fair Credit Reporting Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth; (iv) current address and any previous addresses for the past five (5) years; and (v) any applicable incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

FTC and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. Contact information for the Consumer Response Center of the FTC is 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338) or www.ftc.gov/bcp/edu/microsites/idtheft/.

Protecting Medical Information.

If you are concerned about protecting your medical information, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.