HARDIN COUNTY NOTICE OF DATA SECURITY INCIDENT
November 27, 2024

Hardin County (the "County") has determined that as a result of a recent cyber incident there was unauthorized access and acquisition of personal information maintained in a single County email account. The information included protected health information related to individuals who received services from the County Emergency Medical Services ("EMS") department. **At this time, we are not aware of any misuse of the information involved in this incident**. We take this matter very seriously because of our commitment to the privacy and security of all information. We are providing this notice to inform potentially impacted individuals and suggest ways that individuals can protect their information. On November 27, 2024, we began mailing notifications to individuals whose protected health information and/or personal information was impacted by this incident. Unfortunately, we did not have sufficient contact information to provide written notice to some individuals. We are posting this notice on our website and providing a toll-free telephone number, **866-566-3595**, which can be called 8:00 am and 8:00 pm Central Time (excluding major U.S. holidays), to notify those individuals for whom we do not have sufficient contact information. Please be prepared to provide the following engagement number: **B135668**.

What Happened

On September 26, 2024, the County learned that one County employee email account was being used to send unauthorized spam emails. The County immediately began an investigation, with the assistance of a nationally recognized digital forensics firm, to further understand what happened and to determine the scope of any access to the email account. Through our investigation, we discovered that someone first gained access to the employee's email account on July 1, 2024, and intermittently accessed it between August 1, 2024 and September 26, 2024. During the period of unauthorized access, the contents of the mailbox were downloaded. Once we learned this, we conducted a thorough review of the emails to find out: (1) what information was involved and (2) who may have been affected. On November 15, 2024, we completed our review and began obtaining mailing addresses for impacted individuals to provide them with further details and resources to help protect their personal information. On November 27, 2024, we mailed notice to all impacted individuals for whom we could locate address information.

What Information Was Involved

The County has determined that the data contains the following types of information: name, address, Social Security number, driver's license number, date of birth, information related to medical condition, treatment or diagnosis, name(s) of healthcare provider(s), information regarding services provided to you by Hardin County EMS, such as dates of service, locations of service, case identification number or unique identifiers related to services provided to you, insurance identification number, and/or insurance or billing information.

What We Are Doing About It

Since this incident we have taken steps to ensure the security of all County email accounts. To further strengthen the security of the information we maintain, and to help prevent similar incidents in the future, we have taken the following steps:

1. Secured the impacted email account by changing the password and enhancing its complexity;
2. Strengthened procedure for accessing employee email accounts;
3. Reduced and secured use of personal information for County employee records; and
4. Retrained employee regarding cybersecurity practices related to email.

Additionally, the County has notified the United States Department of Health and Human Services and all appropriate state regulators.

What You Can Do

We recommend that you take the following steps to help protect your information:

1. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements, free credit reports, and any health insurance Explanation of Benefits (EOB) forms for unauthorized or suspicious activity. If you notice any health care services listed in your EOB that you did not receive, you should contact your health plan or doctor. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this notice.

2. Report any incidents of suspected identity theft to your local law enforcement, state Attorney General and the major credit bureaus.

For More Information

Please accept our apology that this incident occurred. We remain fully committed to maintaining the privacy of personal information and will continue to safeguard it.

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit https://www.experian.com/blogs/ask-experian/category/fraud-and-identity-theft/ for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at https://consumer.ftc.gov/features/identity-theft. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

Equifax	**Experian**	**TransUnion**
P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com	P.O. Box 2000 Chester, PA 19016 1-833-799-5355 www.transunion.com

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report. You may be able to obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

Fraud Alerts

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. As soon as one credit bureau confirms the fraud alert, they will notify the others. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. 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 all three of the 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): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement

agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place, you will need it if you choose to lift the freeze.

Protecting Your Medical Information

We have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from 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.

Additional Helpful Information

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them at the information provided above. This notice was not delayed as a result of a law enforcement investigation.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

The County is located at 150 North Provident Way, Elizabethtown, KY 42701. You may also obtain information about preventing and avoiding identity theft from the Kentucky Attorney General's Office. This office can be reached at:

Office of the Attorney General
700 Capital Ave, Suite 118
Frankfort, KY 40601
https://www.ag.ky.gov/
502-696-5300
Consumer Protection Hotline: 888-432-9257