ELMORE COUNTY NOTICE OF DATA SECURITY INCIDENT
JUNE 12, 2025

In connection with a recent cyber incident, Elmore County (the "County") has determined that there was unauthorized access and acquisition of protected health information related to individuals who received services from County Emergency Medical Services. **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 June 13, 2025, we will begin mailing notifications to individuals whose protected health 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, **833-918-1243**, which can be called between 7:00 am and 7:00 pm Mountain 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: **B146836**.

What Happened

On April 15, 2025, the County learned that one employee's email account sent spam emails. We 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 County email accounts. Through our investigation, we discovered that an unauthorized actor accessed some employees' email accounts between April 14, 2025 and April 19, 2025 and that some emails were accessed or downloaded during this time. Once we learned this, we conducted a thorough review of the emails to determine: (1) what information was involved and (2) who may have been affected. On May 12, 2025, we completed the review and began locating address information to provide notice to affected individuals.

What Information Was Involved

The County has determined that the protected health information impacted by this incident included the following: name, date of birth, dates of service, individual identifying number, some medical information, the names of healthcare providers, diagnosis and/or treatment information, laboratory results, and medications related to services received from County Emergency Medical Services.

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 or will be taking the following steps:

1. Securing the impacted email accounts by changing the passwords;
2. Strengthened email access security requirements;
3. Retraining employees regarding cybersecurity practices related to email;
4. Communicating with all staff regarding increased awareness of phishing emails;
5. Enhancing internal policies and procedures related to cybersecurity; and
6. Ongoing investigation of additional tools, training, and third-party monitoring partnerships to strengthen security.

Additionally, the County 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.

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 apologies that this incident occurred. The privacy and security of your information is important to us, and we remain committed to protecting it.