Sabine County HOSPITAL
A MEMBER OF THE PREFERRED FAMILY
2301 Worth Street Hemphill, TX 75948
409-787-3300

You may have recently received notice about a possible security incident from Change Healthcare. More information on this incident and the actions you can take to monitor your credit can be found in the notice below.

Change Healthcare Data Breach Notification

Change Healthcare, a subsidiary of United Healthcare, works with many hospitals, doctors, pharmacies, health insurance plans, and other health companies to process health insurance claims. The company experienced a data breach on February 21, 2024, affecting the personal and health information of as many as 190 million persons, potentially including patients of Sabine County Hospital, Toledo Bend Family Medicine and West Sabine Community Clinic.

Letters regarding the breach have been sent by Change Healthcare to the vast majority of individuals potentially affected, but more may be sent in the ensuing months. For more information about the breach, and to secure free credit monitoring and identity protection services, please use the following link provided by Change Healthcare.

https://url.us.m.mimecastprotect.com/s/_-SnCW6zOqf6xmKg2unsKHoqW_K?domain=click.email.idx.us

---

You may have recently received notice about a possible security incident occurring at Sabine County Hospital. More information on this incident and the actions you can take to monitor your credit can be found in the notice below.

Sabine County Hospital Experiences Information Breach

Hemphill, Texas (August 4, 2025) – Sabine County Hospital (SCH) experienced a security incident in February that may have exposed patient information maintained by the hospital and clinic. .

On February 12, 2025, SCH discovered that an employee's email account had been accessed by an unauthorized individual or entity. The initial investigation revealed that the account was used to send a fraudulent invoice to the hospital. This appears to be the primary objective of the breach.

A thorough and lengthy audit of the compromised account revealed that patient information, contained in internal logs and reports, was present within some of the emails. There is no evidence suggesting that any of this information was accessed or misused. However out of an abundance of caution the hospital has started mailing letters to patients whose information was potentially exposed. A breach notice will also be filed with the Office of Civil Rights.

"We take the privacy of our patients very seriously," said Kaylee McDaniels, RN, hospital administrator, "and took immediate action to secure the affected email account and prevent further access."

In many cases, the information in question was limited to the patient's name, date of service and service received. In other cases, more detailed demographic information such as patient address, date of birth and gender, and clinical information such as symptoms and diagnosis were included. In a limited number of cases, more detailed clinical information regarding tests and treatment, and financial information, such as Social Security number, Medicare number, insurance carrier, and payments made, could also have been viewed.

If you feel you may have been one of these patients or if you received a letter and have questions about the breach, the hospital asks that you call Stacey Ebarb, privacy officer, at 409-787-5005 or toll free at 1-855-730-6680, or send her an email at sebarb@sabinecountyhospital.com.

While the risk of exposure of this information appears very low, the hospital suggests that anyone concerned may wish to take the steps listed on the Federal Trade Commission (FTC) site to protect their identity and reduce any anxiety. The FTC information can also be found on the Sabine County Hospital website: sabinecountyhospital.com.

"Phishing incidents, like the one that occurred at SCH, are becoming increasingly common, and more sophisticated," noted McDaniels. "We are very sorry this occurred, and will continue to educate our staff about the dangers, and steps they should take to avoid becoming a victim.

Federal Trade Commission Identity Protection Recommendations

Anyone who feels their personal information has been stolen may wish to take the following steps from the Federal Trade Commission website to protect their identity.

• **Check credit report to see if an identity thief has used your information.**

Get free credit reports from AnnualCreditReport.com.

Review the reports, and if you see an account or debt you don't recognize, contact the company and ask about it. If someone used information to open a new account or make a purchase, report it at IdentityTheft.gov and learn how to dispute the information on your credit report.

• **Freeze credit to make it harder for someone to use information.** A credit freeze keeps people from getting into a report. While a freeze is in place, nobody can open a new credit account. And it's free to place the freeze, or to temporarily lift the freeze as needed.

Experian.com or call 888-EXPERIAN (888-397-3742)

TransUnion.com or call 888-909-8872

Equifax.com 800-685-1111

• **If you're concerned about identity theft, you can also place a free, one-year fraud alert by contacting one of the three credit bureaus.** A fraud alert makes it harder for someone to open a new credit account in the name of your family member because a business has to verify the identity before it opens the account.

NOTE: You will receive a personal identification number (PIN) to unfreeze your reports in the mail from the credit bureaus – DO NOT LOSE any of these.

• **Keep checking credit reports periodically at AnnualCreditReport.com to watch for anything you don't recognize.** You can check your reports online every week for free.