TEXAS TECH UNIVERSITY
HEALTH SCIENCES CENTER

Return Mail Processing
PO Box 999
Suwanee, GA 30024

75 1 22876 **********AUTO**5-DIGIT 01013
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

June 6, 2022

Dear Sample A. Sample:

Texas Tech University Health Sciences Center (TTUHSC) takes the privacy of our patients seriously, and it is important to us that you are made fully aware of any potential privacy matters. This notification is to inform you of a recent incident with a third-party service provider involving a potential breach of patient information.

What Happened?

Eye Care Leaders, Inc. (ECL) is a third-party service provider of a TTUHSC Electronic Medical Record (EMR) system. On March 28, 2022, TTUHSC was notified that ECL's Integrity EMR application was the subject of a security incident that took place on December 4, 2021, where an unknown attacker accessed and deleted databases and files. ECL reported that it detected the incident in less than twenty-four (24) hours, disabled the attack, and initiated an investigation.

In a letter dated April 19, 2022, ECL informed TTUHSC that it completed its investigation and confirmed that (i) some of the deleted databases and files contained patient records that are Protected Health Information (PHI) and Personally Identifiable Information (PII) and (ii) its forensics team did not find any evidence that PHI or PII of patients was acquired or exfiltrated. However, the possibility could not be definitively ruled out due to insufficient log files. Therefore, as a precautionary measure, we are notifying you of this incident so you can take action to protect your personal information.

ECL has also reported that it informed the FBI of the attack and has stated that it will continue to pursue any domestic or foreign criminal prosecution efforts that are available, if the malicious attacker is identified. TTUHSC is continuing to coordinate with ECL to learn more about the investigation of the incident.

What Information Was Involved?

As reported by ECL, the deleted databases and files may have contained some, or all, of the following personal information:

- Name, address, phone numbers, and email
- Gender, date of birth, driver's license number, and Medical Record Number
- Health insurance information
- Appointment information
- Social Security Number
- Medical information related to Ophthalmology services

The databases and files did not include credit card, bank account, or financial information.

What We Are Doing

ECL reported that it has updated and changed several security features and is working on additional improvements to secure its systems and prevent any future attacks. TTUHSC is also working closely with ECL to mitigate any further risk of exposure. TTUHSC is engaging information technology (IT) experts and legal counsel to properly address and continue to monitor the incident. TTUHSC will also be reporting this incident to the U.S. Department of Health and Human Services and state regulators, as appropriate.

TTUHSC is notifying all affected persons so you can take action to protect your personal information. A toll-free call center is now available, which is operated by Experian, to answer any concerns or questions you may have about this incident. We encourage you to call (855) 891-1998, Monday through Friday, between 8 a.m. and 10 p.m., and Saturday through Sunday, between 10 a.m. and 7 p.m., Central Time. TTUHSC has also arranged for Experian to provide credit monitoring and identity theft protection services at no cost to you. Please review the information and additional resources outlined below.

Enroll in Credit Monitoring

To help protect your identity, TTUHSC is offering a complimentary [Extra1]-month membership to Experian's® IdentityWorks℠. This product provides superior identity theft detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by**: **September 30, 2022** (Your code will be deactivated after this date.)
- **Visit** the Experian® IdentityWorks℠ website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian® IdentityWorks℠ online, please contact Experian's customer care team at (855) 891-1998 by **September 30, 2022.** Be prepared to provide your engagement number **[Engagement Number]** as proof of eligibility for the identity restoration services.

Additional Details Regarding Your [Extra1]-month Experian IdentityWorks℠ Membership:

A credit card is not required for enrollment in Experian® IdentityWorks℠.

You may contact Experian immediately regarding any fraud issues. You also have access to the following features once enrolled in Experian® IdentityWorks℠:

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only. Offline members will be eligible to call for additional reports quarterly after enrolling.
- Credit Monitoring: Actively monitors Experian file for indicators of fraud.
- Internet Surveillance: Technology searches the web, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- Identity Restoration: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARE™: Receive the same high-level of Identity Restoration support even after your Experian IdentityWorks℠ membership has expired.

- Up to $1 Million Identity Theft Insurance: Provides coverage for certain costs and unauthorized electronic fund transfers. The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to specific policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (855) 891-1998. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, assisting you with contacting credit grantors to dispute charges and close accounts; placing a freeze on your credit file with the three major credit bureaus; and contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The terms and conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

You may request free credit reports, place fraud alert or place credit freeze on your credit files at any time by contacting the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
888-298-0045	888-397-3742	833-395-6938
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help

What You Can Do

Although ECL reported that its forensic team has not identified any evidence of data exfiltration, there is insufficient information to conclude that the exfiltration of TTUHSC patients' data could not have occurred during this incident. TTUHSC is not aware of any instances of fraudulent activity connected to this incident; however, as a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained.

TTUHSC has no indication that your personal information has been used to commit fraud, however, we recommend that you consider taking steps to protect yourself from medical identity theft. Medical identity theft occurs when someone uses an individual's name, and sometimes other identifying information, without the individual's knowledge to obtain medical services or products, or to fraudulently bill for medical services that have not been provided. We suggest that you regularly review the explanation of benefits statements that you receive from your health plan. If you see any service that you did not receive, contact the health plan at the number on the statement.

For More Information

TTUHSC is committed to protecting the privacy and security of your personal medical information, and we want to assure you that we have implemented appropriate measures to safeguard that information. We value the trust you have placed in us, and we thank you for trusting TTUHSC with your health care.

Should you have any questions regarding this matter, please do not hesitate to call the toll-free number at (855) 891-1998, Monday through Friday, between 8 a.m. and 10 p.m., and Saturday and Sunday, between 10 a.m. and 7 p.m., Central Time.

Sincerely,

Sonya Castro-Quirino
VP, TTUHSC Institutional Compliance Officer