NOTICE OF DATA PRIVACY INCIDENT

MARCH 18, 2024

ABOUT THE INCIDENT

INTEGRIS Health is making individuals aware of an incident that may affect the privacy of certain information. INTEGRIS Health is providing notice of the event so potentially affected individuals may take steps to better protect their information from misuse, should they feel it appropriate to do so.

FREQUENTLY ASKED QUESTIONS

What Happened? INTEGRIS Health detected suspicious activity within its environment. Upon becoming aware of the suspicious activity, INTEGRIS Health promptly took steps to secure the environment and commence an investigation into the nature and scope of the unauthorized activity. The investigation determined that a file was accessed by an unauthorized party on or about November 28, 2023. INTEGRIS Health then initiated a thorough forensic review to determine the type of information, to whom it related and which healthcare entities were involved. As that review was ongoing, on December 24, 2023, INTEGRIS Health learned that some INTEGRIS Health patients received communications from a group claiming responsibility for the unauthorized access. As a result of its thorough forensic review, INTEGRIS Health determined on or about January 29, 2024, that patient information from IH Community Hospital locations were also included in the accessed files and notified the IH Community Hospitals.

What Information Was Involved? The investigation determined that your name and the following types of personal information were present in the files accessed and/or acquired by the unauthorized actor at the time of the incident: date of birth, contact information, admission and discharge information, demographic information, medical record number, and/or Social Security number. This does NOT involve your electronic health record, employment information, driver's license, credit card or other financial/payment Information, or username/password.

What are We Doing. Upon learning of this incident, INTEGRIS Health promptly assessed the security of its systems, engaged third-party cybersecurity specialists, and implemented security enhancements, including reviewing existing policies and procedures to reduce the likelihood of a similar future incident. INTEGRIS Health continues to monitor its systems and has not observed any further unauthorized activity within its systems and believes that the incident has been contained. As a precautionary measure, we are notifying potentially affected individuals, including you, and to provide peace of mind, offering complementary identity theft and credit monitoring so you may take further steps to better protect your personal information should you feel it is appropriate to do so. These services help detect suspicious activity related to your personal information and provide support in case of identity theft.

What You Can Do. INTEGRIS Health encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and explanation of benefits and monitoring their free credit reports for suspicious activity and to detect errors. Individuals may also review and consider the information and resources outlined in the below "Steps Individuals Can Take to Protect Their Personal Information."

For More Information? If individuals have additional questions, please send an email to INTEGRIS Health at Integrisresponse@integrishealth.org or call our toll-free line at (888) 447-8141.

STEPS INDIVIDUALS CAN TAKE TO PROTECT THEIR PERSONAL INFORMATION

Monitor Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.