INTEGRIS Health – FAQs

1. Who/what is INTEGRIS Health?

INTEGRIS Health is Oklahoma's largest not-for-profit and Oklahoma-owned health care system, with hospitals, specialty clinics, family care practices and centers of excellence.

2. What happened?

INTEGRIS Health discovered potential unauthorized activity on certain systems. Upon becoming aware of the suspicious activity, INTEGRIS Health promptly took steps to secure the environment and commenced an investigation into the nature and scope of the activity. The investigation determined that certain files may have been accessed by an unauthorized party on November 28, 2023. INTEGRIS Health initiated a review of the potentially accessed data to determine the type of information and to whom it related, which is currently underway. On December 24, 2023, INTEGRIS Health learned that patients began receiving communications from a group claiming responsibility for the unauthorized access.

3. How did INTEGRIS Health become aware of the incident?

INTEGRIS Health learned of unusual activity through alerts in its existing security infrastructure, which it promptly began investigating.

4. Was this a ransomware event?

No. There was no encryption or network interruption associated with this event.

5. Was I affected?

INTEGRIS Health is still investigating and currently conducting a detailed review of potentially impacted data to determine the type of information and to whom it relates. However, on December 24, 2023, INTEGRIS Health learned that patients began receiving communications from a group claiming responsibility for the unauthorized access. We encourage anyone receiving such communications do NOT respond or contact the sender, click on any links or downloads, or follow any of the instructions. Instead, please see the steps in the *What You Can Do* section on our website at https://integrisok.com/cyberevent.

6. What Type of Data Was Impacted?

The investigation is ongoing. However, the personal information potentially affected varies by individual but ***may*** include: name, date of birth, contact information, demographic information, and/or Social Security number.

7. What is INTEGRIS Health doing in response to this incident?

As soon as INTEGRIS Health discovered this incident, it promptly took steps to secure its environment and commenced an investigation into the nature and scope of the incident. INTEGRIS Health is also providing information on steps that may be taken to best protect personal information.

8. Is INTEGRIS Health offering monitoring services in connection with this event?

At this time, INTEGRIS Health's investigation into this event remains ongoing. While INTEGRIS Health is not currently offering identity monitoring services, once complete, INTEGRIS Health will be notifying potentially impacted individuals and providing information on steps that may be taken to best protect personal information.

9. What is INTEGRIS Health doing to protect my information?

INTEGRIS Health values and respects the privacy of your information. In response to the incident, INTEGRIS Health is reviewing and enhancing existing safeguards and procedures as part of its commitment to safety. To protect the security of INTEGRIS Health's network, it cannot disclose specific security measures, but please know INTEGRIS Health takes this incident and the security of its networks very seriously.

10. Do you know who is responsible for this?

The party responsible for this activity was not specifically identified. However, on December 24, 2023, INTEGRIS Health learned that patients began receiving communications from a group claiming responsibility for the unauthorized access. We encourage anyone receiving such communications do NOT respond or contact the contact the sender, click on any links or downloads, or follow any of the instructions. Instead, please see the steps in the *What You Can Do* section on our website at https://integrisok.com/cyberevent.

11. Can you provide me more information about this investigation/can I get information from the investigation?

INTEGRIS Health does not have additional information to share regarding the ongoing investigation at this time. We will provide more information when available.

12. There are fraudulent charges on my credit/debit card/financial account. What should I do?

INTEGRIS Health has not identified any potentially impacted data that includes payment information, usernames or passwords or driver's licenses. However, if you observe fraudulent charges on your [credit or debit card / financial account], we encourage you to immediately

contact the issuing financial institution for instructions on how to dispute charges and have a new account issued. Incidents of identity theft and fraud should be reported to law enforcement, your state Attorney General, and the Federal Trade Commission.

13. Someone opened a fraudulent credit card in my name. What should I do?

INTEGRIS Health has not identified any potentially impacted data that includes payment information, usernames or passwords or driver's licenses. However, if an unauthorized credit card has been opened in your name, we encourage you to contact the card's financial institution and report the matter. Incidents of identity theft and fraud should be reported to law enforcement, your state Attorney General, and the Federal Trade Commission.

14. Someone opened a fraudulent loan in my name. What should I do?

INTEGRIS Health has not identified any potentially impacted data that includes payment information, usernames or passwords or driver's licenses. However, if an unauthorized loan has been opened in your name, we encourage you to contact the financial institution servicing the loan and report the matter. Incidents of identity theft and fraud should be reported to law enforcement, your state Attorney General, and the Federal Trade Commission.

15. Does this mean I am a victim of identity theft or fraud?

No, this does not mean that you are the victim of identity theft or fraud. However, if you believe you are a victim of fraud or identify activity within your accounts, there are resources available to you on our website at https://integrisok.com/cyberevent.

16. What is a "fraud alert"?

An initial fraud alert is a 1-year alert that is placed on a consumer's credit file at no cost to the consumer. Upon seeing a fraud alert displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years.

17. What is a Security Freeze?

A security freeze will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan,

credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report.

18. Should I check my credit report?

It is always a good idea to monitor your credit report regardless of whether your information has been involved in an incident. Every U.S. consumer over the age of eighteen can receive one free credit report every twelve months by contacting one of the three national credit bureaus or through the Annual Credit Report Service by visiting www.annualcreditreport.com or calling toll-free, 1-877-322-8228.

19. I think I may be a victim of identity theft. What should I do?

If you believe you are a victim of attempted or actual identity theft or fraud, you can take the following steps:

- Contact appropriate financial institutions to protect or close any accounts that have been tampered with or opened fraudulently.
- Contact the credit reporting agencies to place a "fraud alert" or "security freeze" on your credit reports.
- File a police report and ask for a copy for your records.
- File a complaint with the Federal Trade Commission.
- File a complaint with your state Attorney General.
- Keep good records.
    - Keep notes of anyone you talk to regarding this incident, what he/she told you, and the date of the conversation;
    - Keep originals of all correspondence and forms relating to the suspicious or fraudulent activity, identity theft, or fraud; and
    - Retain originals of supporting documentation, such as police reports and letters to and from creditors. When requested to produce supporting documentation, send copies.
- Keep old files, even if you believe the problem is resolved.