ARMY CRIMINAL INVESTIGATION DIVISION

29 December 2023

Cybercrime Prevention Flyer

Integris Health Data Breach

Integris Health, the largest not-for-profit health care provider in Oklahoma operating 15 hospitals and multiple clinics, is the latest cyberattack victim impacting U.S. Army personnel, dependents, civilians, retirees, and contractors.

An unknown group, initiating the attack on 28 November 2023, exfiltrated the information of more than 2 million patients. Integris Health confirmed the stolen information includes patient names, dates of birth, social security numbers, contact information, and demographic data. Integris Health has said that no usernames/passwords, health information, financial information, or driver's licenses were stolen.

The unknown cyber group demanded payment from Integris Health for the stolen data, but Integris Health refused to pay. Wanting to monetize the stolen information, the unknown group is contacting Integris Health patients by email and demanding a small fee to view or a larger fee to delete the information.

While it may be tempting to pay the ransom, do not do so. There is no guarantee your data will not be released to the public or sold by the attacker to other cybercriminals or scammers. Paying the ransom, making it profitable for the cybercriminals, only encourages future ransomware attacks.

If you are a patient of Integris Health, affiliated with the U.S. Army, and you receive a ransom email demanding payment for your information, notify the Department of the Army Criminal Investigation Division via the Submit a Tip – Report a Crime website. If you are not affiliated with the U.S. Army and receive a ransom email for your Integris Health information, report the incident to the Internet Crime Complaint Center.

Tips for Individuals Impacted by a Data Breach

- **Change passwords.** Use a combination of upper and lowercase letters, numbers, and symbols. Make sure it's not easily guessable, like "password123."
- **Use different passwords.** It is recommended that passwords are not reused for any account.
- **Enroll in two-factor or multi-factor authentication.** This adds an extra layer of security by requiring a second form of verification beyond just your password.
- **Authentication requests.** Do not approve authentication requests you do not recognize.
- **New accounts.** When opening a new account, immediately configure the privacy and security settings.
- **Monitor accounts.** Monitor all accounts for indicators of compromised information.
- **Monitor credit reports.** Obtain free credit reports to identify credit changes or suspicious accounts. Consider placing a free credit freeze or fraud alert notification.
- **Keep software updated.** Software updates fix bugs and resolve security issues.
- **Be suspicious.** Be suspicious of unsolicited phone calls or emails requesting additional information. Do not click on any unknown links or download any unknown files provided in emails.

Additional Resources

Notice of Data Privacy Incident – Integris Health

Learn about your credit report and how to get a copy

Authorized for widest release, without restrictions.

To receive Cyber Directorate Cybercrime Prevention Flyers, send an email to: **CYDIntel@army.mil**

Cyber Directorate Headquarters
Russell Knox Building
27130 Telegraph Road
Quantico, VA 22134

Disclaimer: The appearance of hyperlinks in this Cybercrime Prevention Flyer, along with the views and opinions of authors, products, or services contained therein do not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations.