Notice of Data Privacy Incident

What happened?
Central Texas Pediatric Orthopedics became aware of a security incident occurring on our network on January 25, 2025. We took prompt steps to confirm the security of our systems and initiated a comprehensive investigation to determine the extent of impact to our network. With assistance from a leading forensic security firm, we were able to determine that an unauthorized actor gained access to certain systems from January 23 - 26, 2025. On February 4, we discovered some of the accessed locations likely included patient information and limited information related to volunteers of CTPO. We commenced a thorough review of the files to determine what information was present and to whom the information related. We completed the review, and subsequent address lookup, on April 1, 2025.

Importantly, we have continued caring for patients throughout our response to the incident and all our practices have resumed normal operations.

What information was involved?
The incident may have resulted in unauthorized access to or acquisition of certain folders, files, or records that may have contained one or more of the following data elements: names, dates of birth, passports, and x-ray images.

What are we doing?
CTPO values the privacy and security of our patient and volunteer information. Upon learning about the incident, we immediately launched an investigation with the assistance of a leading outside forensic security firm to determine the nature and scope of the activity and confirm the security of our computer systems and network. We also reported the incident to the FBI.

Out of an abundance of caution, and in accordance with applicable law, we are providing this notice to you so that you can take steps to minimize the risk that your information or your child's information will be misused. We have included a brief description of steps you can take to protect your identity, credit, and personal information.

We have worked diligently to determine how this incident happened and are taking appropriate measures to prevent a similar situation in the future. Since the incident we have implemented a series of cybersecurity enhancements, including installation of additional endpoint detection and response software, resetting all passwords, and rebuilding affected servers. We will continue to assess our policies and procedures already in place for ways to defend against evolving threats.

What can you do?
As with any data incident, we encourage you to remain vigilant for incidents of fraud or misuse from any source and consider taking steps to avoid identity theft, obtain additional information, and protect your personal information. If you find any errors or unauthorized activity, you should contact your financial institution or the appropriate service provider. You may also file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. More steps are described below.

For more information
For additional questions, please feel free to contact the toll-free call center at 1-833-998-9206, Monday through Friday, between 8:00 a.m. and 8:00 p.m. Eastern Time except holidays. You will need to reference the CTPO Incident when calling.

We sincerely apologize for this situation and any inconvenience it may cause you.

ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

Avoiding Medical ID Theft. The following practices can provide additional safeguards to protect against medical identity theft.

- Regularly check the accounts you use regularly to pay for health-related expenses, including bank accounts, health savings accounts, credit card accounts.
- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

Review Personal Account Statements and Credit Reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-888-298-0045	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report Suspected Fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. To place a fraud alert, contact the nationwide credit reporting agencies by phone or online. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- **For Texas Residents:** You can obtain additional information about steps to take to avoid identity theft from the Office of the Attorney General of Texas, PO Box 12548, Austin, TX 78711-2548, 800-621-0508, www.texasattorneygeneral.gov

- **For District of Columbia Residents:** You can obtain additional information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov.

- **For Maryland Residents:** You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.

- **For New Mexico Residents:** You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to http://consumersunion.org/pdf/security/securityNM.pdf

- **For New York Residents:** You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or https://ag.ny.gov/internet/resource-center; or

2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or https://dos.ny.gov/consumer-protection.

- **For North Carolina Residents:** You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

- **For Rhode Island Residents:** You can obtain information from the Rhode Island Attorney General about steps you can take to help prevent identity theft at: 150 South Main Street, Providence, RI 02903, (401) 2744400, www.riag.ri.gov.

- **All U.S. Residents**: The Identity Theft Clearinghouse, Federal Trade Commission may be contacted at 600 Pennsylvania Avenue, NW Washington, DC 20580; 1-877-IDTHEFT (438-4338); and www.consumer.ftc.gov. This notification was not delayed by law enforcement.