

NOTICE OF DATA PRIVACY EVENT

Dr. Stephen Harkins is notifying patients of an incident that may affect the security of some of your personal information. Although there is no indication that your information has been misused in relation to this event, Dr. Stephen Harkins is providing individuals with information about the incident, their response, and resources available to help protect information should individuals feel it necessary to do so. Dr. Stephen Harkins is unaware of any misuse of information in connection with the event and its investigation is still ongoing.

What Happened? On May 19, 2023, our administrative staff and Dr. Stephen Harkins became aware of suspicious activity relating to a cyber incident on our administrative computer systems. Upon discovery of this suspicious activity, Dr. Stephen Harkins launched an investigation to determine the nature and scope of the incident with the assistance of third-party cybersecurity and forensic specialists. Through the investigation we determined that there was unauthorized access to certain computer systems on May 19, 2023. Although the investigation was unable to determine whether specific files were actually accessed or acquired by the threat actor, Dr. Stephen Harkins could not rule out the possibility of such activity. In an abundance of caution, Dr. Stephen Harkins then performed a review of the information contained on that system. This process completed on July 11, 2023. Dr. Stephen Harkins then worked diligently to locate address information for these patients and are providing this notice out of an abundance of caution.

What Information Was Involved? The review determined that the following types of personal information may have been present on the impacted system at the time of the incident: patient names, addresses, dates of birth, Social Security number, telephone numbers, credit card numbers, analysis reports on CT scan imaging performed in our clinic, and the AMA ICD-10/CPT codes for the diagnosis and treatment rendered to each patient. The breached computer server contained patient information utilized in billing and medical insurance claims submission and did not include the detailed medical history information provided during the initial consultations and follow-up office visits.

What We Are Doing. Dr. Stephen Harkins takes this incident and the security of personal information in its care seriously. Upon learning of this incident, Dr. Stephen Harkins moved quickly to investigate and respond to this incident, assess the security of relevant systems, and notify potentially affected patients. Dr. Stephen Harkins also notified and is cooperating with Federal law enforcement. As part of its ongoing commitment to the security of information, Dr. Stephen Harkins is also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

What You Can Do. Dr. Stephen Harkins encourages individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, explanation of benefits, and credit reports for suspicious activity.

For More Information. If individuals have questions about this incident or want additional information, please call the dedicated call center at 1-833-981-4292 from Monday through Friday 8 am – 10 pm CST, or Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays). You may also write to Dr. Stephen Harkins at: 4781 E Camp Lowell Drive, Suite 101, Tucson, AZ 85712.

BEST PRACTICES TO HELP PROTECT PERSONAL INFORMATION

While Dr. Stephen Harkins is unaware of any misuse of personal information as a result of this event, individuals are encouraged to remain vigilant against incidents of identity theft and fraud, to review account statements, explanation of benefits, and to monitor credit reports for suspicious activity and to detect errors. 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.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers’ files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit “prescreened” offers of

credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 2 Rhode Island residents that may be impacted by this event.