2000 Market Street
20th Floor
Philadelphia, PA 19103
215.299.2000 215.299.2150
www.foxrothschild.com

CARLY E. NIXON
Direct No: 215.299.2845
Email: cnixon@foxrothschild.com

May 24, 2024

Washington Attorney General

Via Online Submission Form

Re: **Notice of Data Breach**

To Whom it May Concern:

Our office represents Hypertension-Nephrology Associates, P.C. ("the Practice") and we are writing to provide you with notice of an incident that may affect the personal information of four (4) Washington residents. By providing this notice, the Practice. does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction. The Practice also provided notice to the Department of Health and Human Services pursuant to its HIPAA obligations as a covered entity. The investigation into this incident is ongoing and this notice will be supplemented with any material facts learned subsequent to its submission.

Background

On or around February 6, 2024, the Practice became aware that it was the target of an extortion attack when an extortion note was found on its computer systems. Immediate action was taken, including engaging cybersecurity experts and launching an investigation into the nature and scope of the attack. The investigation revealed the cybercriminal(s) responsible for the extortion attack had accessed the Practice's systems, which contain information on both current and former patients.

The forensic investigation revealed that the cybercriminals accessed the Practice's systems between January 20, 2024, and February 6, 2024. During this time, they exfiltrated data containing patient information. Due to the inability to determine the full extent of the accessed and exfiltrated data, the Practice is treating all information as compromised.

On March 15, 2024, the Practice determined your state resident(s) had their name in addition to one or more of the following data elements impacted: medical diagnosis, medical history and treatment, prescription medication details, laboratory test results, health insurance information, Social Security number and billing information.

Notice to Residents

The Practice mailed written notice of this incident to your state residents between May 14, 2024 and May 17, 2024, in substantially the same form as the letter enclosed.

Steps Taken by the Practice

The Practice reacted immediately upon learning of the attack. In addition to the steps detailed above, the Practice is reviewing its policies and procedures, implemented Multi-Factor Authentication (MFA) on all accounts, and engaged leading cybersecurity experts to effectuate additional safeguards and security protections to better protect against similar incidents in the future. The Practice is offering complimentary credit monitoring and identity restoration services with IDX.

Contact

Should you have any questions regarding notification of other aspects of this incident, please contact me at cnixon@foxrothschild.com or 215-299-2845.

Sincerely,

Carly Nixon

PO Box 480149
Niles, IL 60714

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/hypertension-nephrologyassociates

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

<<May XX, 2024>>

Re: Notice of Security Incident

Dear <<First Name>> <<Last Name>>:

Hypertension-Nephrology Associates, P.C. ("the Practice"), is writing to notify you of a recent incident that may impact your personal information. This letter provides information about the incident, our response, and resources available to you to help protect your personal information, should you feel it necessary to do so.

What Happened? On or around February 6, 2024, the Practice became aware that it was the target of an extortion attack when an extortion note was found on its computer systems. Immediate action was taken, including engaging cybersecurity experts and launching an investigation into the nature and scope of the attack. The investigation revealed the cybercriminal(s) responsible for the extortion attack had accessed the Practice's systems, which contain information on both current and former patients.

What Information Was Involved? In an extortion attack, cybercriminals gain unauthorized access to a victim's sensitive information, such as protected health information (PHI), and then threaten to disclose it unless a ransom is paid. The forensic investigation revealed that the cybercriminals accessed the Practice's systems between January 20, 2024, and February 6, 2024. During this time, they exfiltrated data containing patient information. Due to the inability to determine the full extent of the accessed and exfiltrated data, we are treating all information as compromised. On March 15, 2024, the Practice determined your personal information may have been impacted by this attack. This personal information includes your name, medical diagnosis, medical history and treatment, prescription medication details, laboratory test results, health insurance information, Social Security number and billing information.

What Are We Doing? We take this incident and the security of your information seriously. In addition to the steps detailed above, as part of our ongoing commitment to information security, we are reviewing our policies and procedures, have implemented Multi-Factor Authentication (MFA) on all accounts, and have engaged leading cybersecurity experts to implement additional safeguards and security protections to better protect against similar incidents in the future. We are also offering you <12/24> months of complimentary credit monitoring and identity restoration services with IDX. In addition to notifying you, we also notified law enforcement, applicable federal and state regulators and consumer reporting agencies of this incident as required.

What You Can Do. You can review the enclosed *Steps You Can Take To Protect Your Information*, which contains instructions on how to enroll in the complimentary credit monitoring and identity restoration services. It also includes

additional information on what you can do to better protect against the possibility of identity theft and fraud, if you feel it is appropriate to do so. Please note that while the Practice will cover the cost of IDX's services, you must complete the enrollment process. The enrollment deadline is August 17, 2024.

For More Information. We understand you may have questions that are not answered in this letter. To ensure your questions are answered in a timely manner, please contact our dedicated call center at 1-888-973-9859, which is available Monday through Friday, between 9:00 am and 9:00 pm EST.

We sincerely regret any inconvenience or concern this event has caused you.

Sincerely,

Dr. Inessa Parkansky
Treasurer of Hypertension-Nephrology Associates, P.C.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Website and Enrollment. Scan the QR image or go to https://response.idx.us/hypertension-nephrologyassociates and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring. provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at 1-888-973-9859 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor your accounts: We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity or errors.

Check credit reports. Under United States law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. You may also contact the three major credit bureaus directly to request a free copy of your credit report at:

Equifax	Experian	Transunion
P.O. Box 740256	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 10916
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Place a security freeze. You may place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. You will need to place a security freeze separately with each of the three major credit bureaus if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, contact the credit reporting agencies at:

Equifax	Experian	Transunion
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com/personal/credit-report-services/credit-freeze/	www.experian.com/freeze	www.transunion.com/credit-freeze

Place a fraud alert. At no charge, you can also have the three major credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact the credit reporting agencies.

Review additional resources. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General. You have the right to file a police report if you ever experience identity theft or fraud. This notification was not delayed by law enforcement.

For District of Columbia residents: The Attorney General can be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-727-3400; oag.dc.gov. **For Maryland residents:** The Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, Maryland 21202; 888-743-0023; and https://www.marylandattorneygeneral.gov/. The Practice is located at 735 Fitzwatertown Road Willow Grove, PA 19090. **For New Mexico residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you; the right to know what is in your credit file; the right to ask for your credit score; and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. You have additional rights under the Fair Credit Reporting Act not summarized here and we encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf. **For New York residents:** The Attorney General can be contacted at: Office of the Attorney General, The Capital, Albany, New York 12224; 1-800-771-7755; and ag.ny.gov. **For North Carolina residents:** The Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, North Carolina 27699; 877-566-7226; and www.ncdoj.gov. **For Rhode Island residents**: The Attorney General can be contacted at: 150 South Main Street, Providence, RI 02903; 401-274-4400; and www.riag.ri.gov. A total of X Rhode Island residents may be impacted by this incident.