Aubrey L. Weaver
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
AWeaver@constangy.com
215-770-4234

October 3, 2025

VIA ONLINE SUBMISSION
Attorney General Mike Hilgers
Office of the Attorney General
Consumer Protection Division
2115 State Capital
Lincoln, NE 68509
Email: ago.consumer@nebraska.gov

Re: Notice of Data Security Incident

Dear Attorney General Hilgers:

Constangy, Brooks, Smith & Prophete, LLP, represents Partners in Pediatrics, P.C. ("PIP"), a healthcare provider located in Colorado, in connection with a recent data security incident. PIP takes the protection of all information within its possession very seriously and has taken measures to reduce the likelihood of a similar incident reoccurring. This notice is being sent on behalf of PIP because personal information for one (1) Nebraska resident could have been involved in the data security incident.

1. Nature of the Security Incident

In March 2025, PIP became aware of unusual activity involving a PIP email account and immediately started an investigation using independent experts to assist. The investigation revealed that certain emails within the account could have been accessed or acquired without authorization. PIP thereafter undertook comprehensive review of all potentially affected emails to identify individuals whose information may have been involved and gather contact information needed to provide notice. This process concluded on September 23, 2025, at which time PIP arranged to provide notification.

The potentially affected personal information for the Nebraska resident included the following: name and Social Security number.

2. Number of Nebraska Residents Affected

PIP notified one (1) Nebraska resident within the potentially affected population whose personal information may have been involved on October 3, 2025, via USPS First-Class Mail. A sample copy of the notification letter sent to the potentially affected individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

As soon as PIP discovered the unusual network activity, it took steps to secure the affected email account and launched an investigation to learn more about what happened and what information could have been involved. PIP is further reviewing existing policies and procedures and implementing enhanced security measures to reduce the likelihood of a similar incident occurring in the future

PIP has established a toll-free call center through Epiq to answer questions about the incident and address related concerns. Additionally, PIP is providing notified individuals whose Social Security numbers may have been involved with twelve (12) months of free credit monitoring and identity protection services through Experian.

4. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at 215-770-4234 or aweaver@constangy.com.

Sincerely,

Aubrey L. Weaver
Partner, Constangy Cyber Team

Attachment: Sample Notification Letter

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Subject: Notice of Data Security Incident

Dear <<Full Name>>,

We are writing to inform you of a recent data security incident that may have involved your information. Partners in Pediatrics ("PIP") takes the privacy and security of all information in our possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your information.

What Happened. We recently learned that some of your personal information was involved in data security incident. We experienced unusual activity involving a PIP email account on March 5, 2025, and immediately started an investigation using independent experts to assist. We later learned that some emails within the account could have been accessed or acquired without authorization in March 2025. We then worked to determine whose information was potentially involved in the incident, which process concluded on September 23, 2025.

Please note that this incident was limited to information transmitted via email and did not involve our electronic health records or other PIP information systems. We have no evidence of the misuse of anyone's information.

What Information Was Involved. The potentially involved information varies by individual. Based on the investigation, we understand that the information may have included your <<Breached Elements>>.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. As part of our ongoing commitment to information security, we are reviewing existing policies and procedures and implementing enhanced security measures to reduce the likelihood of a similar incident occurring in the future. We are further notifying you of this event and advising you about steps you can take to help protect your information.

Additionally, to help protect your information, we are offering complimentary access to Experian IdentityWorks^{SM} for 12 months. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by **<<Enrollment Deadline>>** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: **<<Activation Code>>**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057 by **<<Enrollment Deadline>>**. Be prepared to provide engagement number **<<Engagement Number>>** as proof of eligibility for the Identity Restoration services by Experian.

What You Can Do. You can follow the recommendations on the following page to help protect your information. We also encourage you to take advantage of the complimentary identity protection services being offered.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call our dedicated team at 855-291-2707, Monday through Friday from 6:00 am – 6:00 pm Mountain Time. Representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your information.

Please be assured that PIP takes the privacy and security of all information within our possession very seriously. We hope you will accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Partners in Pediatrics, P.C.
3801 E. Florida Avenue, Suite 300
Denver, Colorado 80210

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Internal Revenue Service Identity Protection PIN (IP PIN): You may obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service – a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Information about the IP PIN program can be found here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	**Experian** P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	**TransUnion** P.O. Box 2000 Chester, PA 19016 1-833-799-5355 www.transunion.com/get-credit-report

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

Security Freeze: You have the right to put a security freeze on your credit file at no cost. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. For TransUnion: www.transunion.com/credit-freeze.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov 877-438-4338	**Maryland Attorney General** 200 St. Paul Place Baltimore, MD 21202 www.marylandattorneygeneral.gov/Pages/CPD 888-743-0023	**Oregon Attorney General** 1162 Court St., NE Salem, OR 97301 www.doj.state.or.us/consumer-protection 877-877-9392

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.