Donna Maddux, Partner
Cybersecurity & Data Privacy Team
4800 SW Meadows Road,
Suite 300
Lake Oswego, Oregon 97035
dmaddux@constangy.com
Direct: 503.376.5939

February 27, 2025

VIA ONLINE SUBMISSION
Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: **Carolina Arthritis Associates – Preliminary Notice of Data Security Incident**

Attorney General Frey:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents Carolina Arthritis Associates ("Carolina Arthritis"), a rheumatology practice located at 1710 South 17th Street Wilmington, North Carolina, in connection with the data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with the Maine data breach notification statute.

1. **Nature of the Security Incident**

On September 27, 2024, Carolina Arthritis experienced a computer network disruption. Carolina Arthritis immediately took steps to secure its systems and engaged cybersecurity experts to conduct an investigation to determine what happened. The investigation determined that certain files may have been acquired without authorization on or about September 27, 2024. With assistance of additional experts, Carolina Arthritis then undertook a comprehensive programmatic and manual review of the affected data. Carolina Arthritis determined on January 21, 2025 that certain individual information was potentially affected.

2. **Number of Affected Maine residents & Information Involved**

The incident involved personal information for three (3) Maine residents. The information involved in the incident for the affected Maine residents may have included their Date Of Birth, Medical Treatment Or Procedure Information, Medical Record Number, Medical Provider Name, And Social Security Number. Written notice is being provided in substantially the same for as the letter attached here as ***Exhibit A.***

3. Notification to the Affected Individual

On February 27, 2025, a notification letter was mailed to the affected Maine residents by USPS First Class Mail. The notification letter provides resources and steps this individual can take to help protect their information. The notification letter also offers individuals with Social Security number and/or driver's license potentially impacted the opportunity to enroll in 12 months of complimentary identity protection services, including credit monitoring, and identity remediation services, as well as access to a call center for 90 days, should the individual have questions about the incident. Those services are offered by CyberScout, a TransUnion company specializing in fraud assistance and remediation services. A sample notification letter sent to the impacted individual is included with this correspondence.

4. Steps Taken Relating to the Incident

In response to the incident, Carolina Arthritis retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Carolina Arthritis also implemented additional security measures to further harden its environment in an effort to prevent a similar event from occurring in the future. Finally, Carolina Arthritis is notifying the affected individual and providing them with steps they can take to protect their personal information as discussed above.

5. Contact Information

Carolina Arthritis remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Donna Maddux at dmaddux@constangy.com.

Sincerely,

Donna Maddux
Constangy, Brooks, Smith & Prophete, LLP

Encl.: Exhibit A: Sample Notification Letter

Carolina Arthritis Associates
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

Carolina Arthritis

February 27, 2025

Subject: Notice of Data Security Incident

Dear [redacted],

Carolina Arthritis Associates ("Carolina Arthritis") is writing to inform you of a data security incident that may have involved your personal information. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened? On September 27, 2024, Carolina Arthritis experienced a computer network disruption. We immediately took steps to secure our network environment and engaged cybersecurity experts to conduct an investigation to determine what happened. The investigation determined that certain files may have been acquired without authorization on or about September 27, 2024. We then conducted a comprehensive review of the affected data to determine whether personal information may have been involved. After a thorough review of the impacted data, on January 21, 2025, it was determined that some of your personal information was present in the impacted data set. Carolina Arthritis has no evidence of the misuse of any involved data.

What Information Was Involved? The information involved may include your name and [redacted]

What We Are Doing. As soon as we discovered the incident, we took the steps described above. We also reported the incident to the FBI and will cooperate with any resulting investigation. Additionally, we implemented measures to reduce the risk of a similar incident occurring in the future.

We are also providing you with access to Single Bureau Credit Monitoring, Single Bureau Credit Report, Single Bureau Credit Score services, identity protection services, identity resolution services, and a $1,000,000 identity theft insurance policy at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted].

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the Cyberscout identity protection services, which are offered at no cost to you.

For More Information. If you have questions about this letter or need assistance, please call our dedicated team with Cyberscout at 1-833-799-3772. Cyberscout representatives are available Monday through Friday from 8:00 am - 8:00 pm Eastern Time, excluding holidays. Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

We take this event and the security of information in our care seriously. Please accept our sincere apologies and know that we deeply regret any concern or inconvenience that this may cause you.

Sincerely,

Carolina Arthritis Associates
1710 South 17th Street
Wilmington, NC 28401

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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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 (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

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 http://www.annualcreditreport.com/, calling toll-free 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 can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 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, 833-799-5355 , www.transunion.com/get-credit-report.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report--an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the FTC identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security 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. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; http://oag.ca.gov/

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; https://www.maine.gov/ag/

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; https://ag.ny.gov/

Oregon: Oregon Office of the Attorney General can be reached at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR, 97301, 1-877-877-9392, www.doj.state.or.us

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, http://www.riag.ri.gov. The total number of Rhode Island residents receiving notification of this incident is 1.

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov