Laura K. Funk, Partner
Cybersecurity & Data Privacy Team
1201 Elm Street, Suite 2550
Dallas, Texas 75270
LFunk@constangy.com
Mobile: 248.709.9385

June 26, 2024

**VIA ONLINE SUBMISSION**
Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

**Re: Notification of Data Security Incident**

Dear Attorney General Frey:

Constangy Brooks Smith & Prophete LLP represents The Mount Kisco Surgery Center LLC d/b/a The Ambulatory Surgery Center of Westchester ("ASCW"), located in New York, with respect to a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident.

**Nature of the Security Incident**

On November 3, 2023, ASCW discovered unusual activity in one employee's email account. Upon discovering this activity, it immediately took steps to secure the account. It also engaged a digital forensics and incident response firm to conduct an investigation to determine whether any data within the mailbox may have been affected. The investigation revealed that certain emails within the employee's account may have been accessed or acquired without authorization between October 23, 2023, and November 3, 2023.

ASCW then undertook a comprehensive review of the potentially affected data. On May 30, 2024, it identified that certain individuals' personal and/or protected health information was contained in the mailbox. The affected information varies by individual, but may have included individuals' names, Social Security numbers, driver's license or state identification numbers, dates of birth, medical information, including diagnosis information, treatment information, and prescription information, and health insurance information, including claim information and health insurance ID numbers, and financial account information.

**Number of Maine Residents Affected**

On June 26, 2024, ASCW notified thirteen (13) Maine residents of this incident via First-Class U.S. mail. A sample copy of the notification letter sent to impacted individuals is included with this correspondence.

**Steps Taken Relating to the Incident**

To help prevent something like this from happening again, ASCW is implementing additional security protocols. It is also offering complimentary credit and identity protection monitoring services to all individuals whose Social Security numbers were potentially affected by the incident.

**Contact Information**

ASCW remains dedicated to protecting the information in its possession. If you have any questions or need additional information, please do not hesitate to contact me by phone at 248.709.9385 or by email at lfunk@constangy.com.

Regards,

Laura K. Funk
Partner

Enc.: Sample Consumer Notification Letter

Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

June 26, 2024

**Re: Notice of Data <<Security Incident/Breach>>**

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

We are writing to inform you of a data security incident that may have affected your personal and/or protected health information. At The Mount Kisco Surgery Center LLC d/b/a The Ambulatory Surgery Center of Westchester ("ASCW"), we take the privacy and security of personal and/or protected health information very seriously. That is why we are notifying you of the incident, providing you with steps you can take to help protect your information, and offering you complimentary identity protection services.

**What Happened.** On November 3, 2023, ASCW discovered unusual activity in one employee's email account. Upon discovering this activity, we immediately took steps to secure the account. We also engaged a digital forensics and incident response firm to conduct an investigation to determine whether any data within the mailbox may have been affected.

The investigation revealed that certain emails within the employee's account may have been accessed or acquired without authorization between October 23, 2023, and November 3, 2023. ASCW then undertook a comprehensive review of the potentially affected data. On May 30, 2024, we identified that some of your personal and/or protected health information was contained in the account. Since then, we have been working to gather contact information necessary to provide you with this notice.

**What Information Was Involved**. The potentially affected information may have included your name and <<Data Elements>><<Data Elements Continue>>

**What We Are Doing.** As soon as ASCW discovered the incident, we took the steps described above. We also implemented additional measures to enhance our email security and minimize the risk of a similar incident occurring in the future. As a further precaution, we are offering you <<12/24>> months of complimentary identity protection services through IDX. This product helps detect possible misuse of your information and provides you with identity protection support.

**What You Can Do.** We encourage you to review the recommendations included with this letter to help protect your information. In addition, you can also enroll in IDX's complimentary identity protection services by going to the link noted above or calling the number noted above. When prompted, please provide the unique code noted above to enroll in the services. The deadline to enroll is September 26, 2024. For more information on how you can protect your personal information, please review the resources provided on the following pages.

**For More Information.** If you have questions or need assistance, please call 1-888-715-8252 Monday through Friday from 9 am to 9 pm Eastern.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

The Ambulatory Surgery Center of Westchester
34 S Bedford Road
Mount Kisco, NY 10549

## STEPS YOU CAN TAKE TO 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 (FTC).

**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 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
1-800-916-8800
www.transunion.com

**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 http://www.annualcreditreport.com.

**Security Freeze:** You have the right to put a security freeze on your credit file for up to one year at no cost. This 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. 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.

**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, and
www.ftc.gov/idtheft
1-877-438-4338

**Maryland Attorney General**
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

**New York Attorney General**
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

**North Carolina Attorney General**
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

**Rhode Island Attorney General**
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

**Washington D.C. Attorney General**
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

**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 https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

A total of 21,073 individuals were notified of this incident.