



Donna Maddux, Partner
Cybersecurity & Data Privacy Team
4800 SW Meadows Road, Suite 300
Lake Oswego, Oregon 97035
Telephone: 503.312.6251
Email: dmaddux@constangy.com

February 8, 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
Tel: 207-626-8800

Re: **Notice of Data Security Incident**

Attorney General Frey:

Constangy, Brooks, Smith & Prophete, LLP (“Constangy”) represents Memorial Hospital and Manor (“Memorial”) in connection with a data security incident described in greater detail below. Memorial is an independent community hospital located in Bainbridge, Georgia. The purpose of this letter is to notify you of the impact to Maine residents in accordance with the Maine data breach notification statute.

1. Nature of the Security Incident

On November 2, 2024, Memorial became aware of unusual activity that disrupted access to certain computer systems. Upon discovery, Memorial immediately took steps to secure its network and engaged a leading, independent cybersecurity firm to investigate what happened and whether any sensitive data may have been impacted. The investigation subsequently revealed certain personal information and personal health information was accessed and acquired without authorization by an unknown actor during the incident. Memorial undertook a comprehensive review of the potentially impacted data to identify the individuals and information involved, including address information for mailing purposes. That process concluded on January 31, 2025. Memorial then took steps to notify impacted consumers of the incident as quickly as possible.

Please note that Memorial has no current evidence to suggest misuse or attempted misuse of personal information involved.

2. Number of Affected Maine Residents & Information Involved

The incident involved personal information for approximately 3 Maine residents. The information involved in the incident may have included individuals' names, Social Security numbers, dates of birth, health insurance information, and medical treatment and/or history information.

3. Notification of Affected Individuals

On February 7, 2025, notification letters were mailed to affected Maine residents by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers 12 months of complimentary identity protection services to each individual whose personal information was affected by this event, including credit monitoring, \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Those services are offered by IDX – a data breach and recovery services expert. These services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

3. Steps Taken to Address the Incident

In response to the incident, Memorial retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Memorial also implemented additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future.

Finally, Memorial is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above.

4. Contact Information

Memorial remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at DMaddux@Constangy.com or 503.312.6251.

Sincerely,



Donna Maddux of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Consumer Notification Letter



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:



Or Visit:

<https://response.idx.us/MemorialHospitalandManor>

February 7, 2025

Subject: Notice of Data <<Variable Text 1: Security Incident / Breach>>

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

We are writing to inform you about a recent data security incident experienced by Memorial Hospital and Manor (“Memorial”) 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 personal information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened? On November 2, 2024, Memorial became aware of unusual activity that disrupted access to certain computer systems. Upon discovery, we immediately took steps to secure our network and engaged a leading, independent cybersecurity firm to investigate what happened and whether any sensitive data may have been impacted. The investigation subsequently revealed certain personal information and personal health information was accessed and acquired without authorization by an unknown actor during the incident. Memorial undertook a comprehensive review of the potentially impacted data to identify the individuals and information involved, including address information for mailing purposes. That process concluded on January 31, 2025. We then took steps to notify you of the incident as quickly as possible.

What Information Was Involved? The information impacted during this incident may have included your name, Social Security number, date of birth, health insurance information, and medical treatment and/or history information.

What We Are Doing. As soon as Memorial discovered the incident, we took steps to secure our environment and enlisted a leading, independent cybersecurity firm to conduct a forensic investigation. We also reported the incident to the FBI and will cooperate with any resulting investigation. In addition, we have implemented several measures to enhance our security posture and reduce the risk of similar future incidents.

We are also offering you access to complimentary credit monitoring and identity theft protection services through IDX – a data breach and recovery services expert. These services include: <<12/24>> months of credit¹ and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

¹To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

To enroll, please call 1-877-608-6023 or visit <https://response.idx.us/MemorialHospitalandManor> and provide the enrollment code at the top of this page. Please note you must enroll by May 7, 2025. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

What You Can Do. We encourage you to enroll in the credit protection services we are offering, which are at no cost to you. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

For More Information: If you have questions or need assistance, please contact 1-877-608-6023 Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Sincerely,

Memorial Hospital and Manor

1500 E Shotwell St
Bainbridge, GA 39819

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Financial Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your financial account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect financial accounts, including promptly changing passwords. If you detect any suspicious activity on a financial account, you should promptly notify the financial institution or company with which the financial 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 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

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 proof. 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

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