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

May 12, 2025

VIA ONLINE SUBMISSION
Attorney General Nick Brown
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100
Email: SecurityBreach@atg.wa.gov

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP, represents Weiser Memorial Hospital ("WMH"), a hospital located in Weiser, Idaho. WMH 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 WMH because personal information for 1163 Washington residents could have been involved in the data security incident.

1. Nature of the Security Incident

On September 4, 2024, WMH became aware of unusual network activity and immediately took steps to secure our systems. We engaged cybersecurity experts to assist with the process. The investigation determined that certain WMH data may have been acquired without authorization on or about September 4, 2024. As a result, WMH undertook a comprehensive review of all potentially affected files to try and identify individuals whose information may have been involved and gather contact information needed to provide notice. These efforts concluded on April 21, 2025, at which time WMH arranged to provide notice to all potentially affected individuals.

The potentially affected personal information may have included individuals' names, Social Security numbers, health information, and/or health insurance information.

2. Number of Washington Residents Affected

WMH notified 1163 Washington residents within the potentially affected population on May 12, 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 WMH discovered the unusual network activity, it took steps to secure its systems and launched an investigation to learn more about what happened and what information could have been affected. WMH has implemented additional safeguards to enhance the security of its systems and to reduce the risk of a similar incident occurring in the future.

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

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

Weiser Memorial Hospital
c/o Cyberscout
<Return Address>
<City> <State> <Zip>

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

Date

<<Custom Field 1>>

Dear <<FirstName>> <<LastName>>,

We are writing to inform you of a data security incident that may have affected your personal or protected health information. Weiser Memorial Hospital ("Weiser") takes the privacy and security of all information in our possession very seriously. This letter has information about the incident and steps you can take to protect your information, including enrolling in the complimentary credit monitoring and identity protection services we are making available to you.

What Happened. On September 4, 2024, Weiser became aware of unusual network activity and immediately took steps to secure our systems. We engaged cybersecurity experts to assist with the process. The investigation determined that certain Weiser data may have been acquired without authorization on or about September 4, 2024. As a result, Weiser undertook a comprehensive review of all potentially affected files to try and identify individuals whose information may have been involved and gather contact information needed to provide notice. These efforts concluded on April 21, 2025. After we learned that some of your information was potentially involved, we arranged to provide you with this notice.

What Information Was Involved. The potentially affected information may have included your <<Exposed Data Elements>>.

What We Are Doing. As soon as Weiser discovered the incident, we took the steps described above and implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future.

Additionally, to help relieve concerns and to help protect your information following this incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for <<Service Length>> from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. 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: <Unique Code>

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. We encourage you to you activate your complimentary credit monitoring services using the enrollment code provided above, and to review any account statements and explanation of benefits forms and report any errors or activity you do not recognize to your insurance carrier. We also recommend that you review the guidance included with this letter about additional steps you can take to protect your information.

For More Information. If you have any questions about this letter, please contact our dedicated team with Cyberscout for this incident at 1-833-799-3704. Representatives have been fully versed on the incident and are available Monday through Friday from 8:00 am to 8:00 pm EST (excluding major U.S. holidays).

Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Weiser Memorial Hospital
645 E. 5th St
Weiser, ID 83672

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").

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
1-800-916-8800
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 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
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

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

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

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

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

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

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.