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

March 28, 2025

VIA ONLINE SUBMISSION
Attorney General Bob Ferguson
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 Ferguson:

Constangy, Brooks, Smith & Prophete, LLP, represents Montana Health Solutions ("MHS"), a caregiving, nursing, and personal emergency response services provider based in Montana. MHS 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 MHS and its covered entity partners because personal information for 619 Washington residents could have been involved in the data security incident.

1. Nature of the Security Incident

On September 17, 2024, MHS learned of activity related to an employee email account. MHS took steps to investigate and learned that some data could have been viewed without authorization. MHS then took steps to review the data that could have been involved. At the end of the review, on January 8, 2025, MHS provided notification to its partner organizations and worked with them to effectuate notice. This process concluded on February 21, 2025.

The potentially affected information may have included individuals' names, Social Security number, driver's license information, financial account information, diagnosis or treatment information, and/or other health- or employment-related information.

2. Number of Washington Residents Affected

MHS notified 619 Washington residents within the potentially affected population on March 19, 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 MHS 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. MHS has implemented additional safeguards to enhance the security of its systems and to reduce the risk of a similar incident occurring in the future.

MHS has established a toll-free call center through Epiq to answer questions about the incident and address related concerns. Additionally, MHS is providing notified individuals with free Experian identity protection services. These identity protection services include complimentary access to Experian IdentityWorksSM for 12 months.

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

Montana Health Solutions ("MHS")
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>>,

I am writing to inform you of an incident experienced by Montana Health Solutions ("MHS") that may have involved some of your information. If you are not familiar with MHS, we work with companies, including <<Variable Data 1>>, to provide services related to in-home care assistance. MHS is committed to the privacy and security of all information in our possession. This letter includes information about the incident and provides you with steps you can take to protect your information.

What happened? On September 17, 2024, MHS learned of activity related to an employee email account. MHS took steps to investigate and learned that some data could have been viewed without authorization. MHS then took steps to review the data that could have been involved. At the end of the review, on January 8, 2025, we provided notification to the companies we work with, including <<Variable Data 1>>, and worked with them to provide you with this notice.

What Information Was Involved? The potentially affected information included your <<Breached Elements>>.

In addition, to help protect your information, we are offering complimentary access to Experian IdentityWorks^{SM} for 12 months. Additional information about Experian IdentityWorks^{SM} and how to enroll is included with this letter.

What We Are Doing: As soon as MHS discovered the incident, we took the steps described above. We also performed a thorough review of our systems to investigate the incident and ensure that our systems remain secure. MHS also implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents.

What You Can Do: We recommend that you review the guidance included with this letter with best practices for how to protect your information.

For More Information: If you have any questions about this letter, please contact our dedicated call center for this incident at 1-855-659-0107 toll-free Monday through Friday from 7 am – 7 pm Mountain time (excluding major U.S. holidays).

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Montana Health Solutions
100 Consumer Direct Way
Missoula, Montana 59808

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR 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 1000
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

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

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

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

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

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

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

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

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.

INFORMATION REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

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.

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.