



Laura Funk, Partner
Cybersecurity & Data Privacy Team
100 Crescent Court, Suite 700
Dallas, Texas 75201
Telephone: 248.709.9385
Email: lfunk@constangy.com

July 17, 2025

VIA Online Submission

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capital
Lincoln, NE 68509
Tel: 402-471-2683

Re: **Notice of Data Breach**

Dear Attorney General Hilgers

Constangy, Brooks, Smith & Prophete, LLP (“Constangy”) represents Western Montana Mental Health (“WMMHC”) in connection with a data security incident described in greater detail below. The purpose of this letter is to notify you of the impact to Nebraska residents in accordance with Nebraska’s data breach notification statute.

Nature of the Security Incident

On September 15, 2024, WMMHC discovered that it was experiencing a network disruption and immediately initiated an investigation of the matter with the assistance of independent cybersecurity experts. As a result of the investigation, WMMHC determined that certain files were accessed without authorization. WMMHC then engaged a third-party data review team to conduct a comprehensive review of those files, and, on or about May 27, 2025, learned that personal and protected health information belonging to WMMHC was contained within the potentially affected data.

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

Number of Affected Nebraska Residents & Information Involved

The incident involved personal information for approximately 10 Nebraska residents. The information involved in the incident may have included individuals’ names, Social Security numbers, driver’s license numbers, dates of birth, state or federal identification numbers, medical information, financial account information, and/or health insurance information.

Notification of Affected Individuals

On July 17, 2025, notification letters were mailed to affected Nebraska 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 Social Security number was potentially affected by this event, which includes 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.

Steps Taken to Address the Incident

In response to the incident, WMMHC retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. WMMHC 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, WMMHC is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above.

Contact Information

WMMHC 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 lfunk@constangy.com.

Sincerely,



Laura Funk of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Consumer Notification Letter



P.O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

July 17, 2025

Subject: Notice of Data [Variable Text 1: Security Incident / Breach]

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

I am writing to inform you of a recent data security incident that may have affected your personal or protected health information. Western Montana Mental Health Center (“WMMHC”) takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your information.

What Happened. On September 15, 2024, WMMHC discovered that it was experiencing a network disruption and immediately initiated an investigation of the matter with the assistance of independent cybersecurity experts. As a result of the investigation, we determined that certain files were accessed without authorization. WMMHC then engaged a third-party data review team to conduct a comprehensive review of those files, and, on or about May 27, 2025, we learned that personal and protected health information belonging to WMMHC was contained within the potentially affected data.

What Information Was Involved. The information may have included your name and your [Additional Data Elements]. Please note that WMMHC has no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What We Are Doing. As soon as WMMHC discovered this incident, we took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. WMMHC also notified the Federal Bureau of Investigation and will cooperate with any resulting investigation. WMMHC is also offering you complimentary identity protection services through IDX, a leader in consumer identity protection. These services include <<12/24>> months of credit monitoring, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. The deadline to enroll in these services is October 17, 2025.

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 complementary services offered to you through IDX by using the enrollment code provided above.

For More Information. Further information about how to protect your personal and protected health information appears on the following page. If you have questions or need assistance, please call 1-855-202-1403 Monday through Friday from 9am-9pm ET. 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,
Western Montana Mental Health Center

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 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.

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
ag.ny.gov
800-771-7755

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

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.

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.