



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

March 18, 2024

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Weirton Medical Center (“Weirton”) located at 601 Colliers Way, Weirton, WV 26062, and are writing to notify your office of an incident that may affect the security of certain personal information relating to two (2) New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Weirton does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On January 18, 2024, Weirton discovered suspicious activity in its network. Weirton immediately took steps to secure its systems and launched an investigation into the nature and scope of the event with the assistance of third-party forensic specialists. The investigation determined that between January 14, 2024, and January 18, 2024, an unknown actor gained access to certain systems on Weirton’s network and acquired certain files from these systems. In response, Weirton thoroughly reviewed the affected files in order to identify what information is contained therein and to whom that information relates. On March 6, 2024, Weirton completed its comprehensive review and confirmed that information relating to certain current and former patients was present in the affected files. Weirton does not have evidence of any actual or attempted fraudulent misuse of information as a result of this incident.

The type of information affected by this event includes

Notice to New Hampshire Residents

On March 18, 2024, Weirton provided written notice of this incident to two (2) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Weirton moved quickly to investigate and respond to the incident, assess the security of Weirton's systems, and identify potentially affected individuals. Further, Weirton notified federal law enforcement regarding the event. Weirton is also working to implement additional safeguards and training to its employees. Weirton is providing access to credit monitoring services for [redacted] through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Weirton is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Weirton is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Weirton is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Weirton is also notifying the U.S. Department of Health and Human Services and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at [redacted].

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD/kgf
Enclosure

EXHIBIT A



Return Mail Processing
PO Box 999
Suwanee, GA 30024

104 1 26724 *****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



March 18, 2024

NOTICE OF [Extra1]

Dear Sample A. Sample,

Weirton Medical Center (“Weirton”) is writing to inform you of a recent incident that impacted the privacy of some of your information. While we are unaware of any misuse of your information, we are providing you with information about the event, our response to it, and resources we are making available to you to help protect your information should you wish to do so.

What Happened? On January 18, 2024, we discovered suspicious activity in our network. We immediately took steps to secure our systems and launched an investigation into the nature and scope of the event with the assistance of third-party forensic specialists. The investigation determined that between January 14, 2024, and January 18, 2024, an unknown actor gained access to certain systems on our network and acquired certain files from these systems. In response, we thoroughly reviewed the affected files in order to identify what information is contained therein and to whom that information relates. On March 6, 2024, we completed our comprehensive review and confirmed that information relating to certain current and former patients was present in the affected files, including you.

What Information Was Involved? While we have no evidence of any actual or attempted fraudulent misuse of information as a result of this incident, our review determined that the following types of information were present in the affected files: your [Extra2]. **Please note that our electronic medical record (EMR) system is not hosted within Weirton’s network and was not impacted by this event.**

What We Are Doing. The confidentiality, privacy, and security of personal information is among Weirton’s highest priorities, and we have strict security measures in place to protect information in our care. Upon becoming aware of this incident, we immediately took steps to secure our systems and launched a full investigation with the assistance of third-party forensic specialists. Since discovering the event, we have implemented additional security measures to further protect against similar incidents occurring in the future. We also reported this incident to federal law enforcement and applicable regulators, including the U.S. Department of Health and Human Services.

Additionally, we are offering credit monitoring and identity protection services for [Extra3] months through Experian, at no cost to you. The deadline to enroll in these services is . Please note that you will not be automatically enrolled in these services. Should you wish to do so, you will need to enroll yourself in these services, as we are not able to do so on your behalf. You may find instructions on how to enroll in these services in the enclosed *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information*. There you will also find more information on the credit monitoring and identity protection services we are making available to you, free of cost.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions or need assistance, please call our dedicated assistance line at 833-918-8051 between the hours of 9:00 a.m. and 9:00 p.m., Eastern Time, Monday through Friday, excluding major U.S. holidays. You may also write to Weirton at 601 Colliers Way, Weirton, WV 26062.

We sincerely regret any inconvenience or concern this incident may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

Weirton Medical Center

Steps You Can Take to Help Protect Personal Information

Enroll in Credit Monitoring and Restoration

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for [Extra3] months.

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 [Extra3] 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 [variable text 3]-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:

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 [Customer Care Phone Number]. Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra3]-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 file 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.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

| Equifax | Experian | TransUnion |
|---|---|---|
| https://www.equifax.com/personal/credit-report-services/ | https://www.experian.com/help/ | https://www.transunion.com/credit-help |
| 1-888-298-0045 | 1-888-397-3742 | 1-800-916-8800 |
| Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 | Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 | TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 |
| Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788 | Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013 | TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094 |

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There is approximately 2 Rhode Island resident that may be impacted by this event.