M. Alexandra Belton
Office: (267) 930-4773
Fax: (267) 930-4771
Email: abelton@mullen.law

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

October 9, 2025

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 Coos County Family Health Services ("Coos County") located at 133 Pleasant Street, Berlin, NH 03570, and write to notify your office of an incident that may affect certain personal information relating to approximately thirty-five thousand six hundred nine (35,609) New Hampshire residents. By providing this notice, Coos County 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 July 9, 2025, Coos County became aware of suspicious activity related to its phone systems and servers. Coos County began an investigation to determine the nature and scope of the activity and took steps to secure its systems. The investigation determined that there was unauthorized access to the servers on July 9, 2025, during which an unauthorized party may have viewed or copied data. In an abundance of caution, Coos County reviewed the files that may have been impacted and, on August 12, 2025, confirmed they contained patient information. Coos County then worked to reconcile the individual records and determine contact information for patients. This involved extensive internal data review and reconciliation to identify individuals, confirm the legitimacy of the records, deduplicate records, and validate contact information in furtherance of determining the notice population. This process was completed on or around September 26, 2025. Coos County then worked with a notification vendor to validate contact information and on, October 2, 2025, it was determined that notice would be provided to approximately thirty-five thousand six hundred nine (35,609) New Hampshire residents. The information related to New Hampshire residents that was found in the relevant files includes names, dates of birth, contact information, Social Security numbers, medical identification numbers and medical information.

Notice to New Hampshire Residents

On or around September 5, 2025, while its investigation was ongoing, Coos County posted notice of this incident to its website. On or about October 9, 2025, Coos County will provide written notice of this incident to 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

In response to this incident, Coos County took steps to secure its systems and conduct a thorough investigation. Further, Coos County notified federal law enforcement. Coos County is notifying potentially affected individuals and providing guidance on how to better protect against identity theft and fraud, as demonstrated in the attached ***Exhibit A***. Coos County is also providing notified individuals with access to credit monitoring services for twelve (12) months, through TransUnion. Additionally, Coos County is providing written notice of this incident to relevant state regulators, as appropriate, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Coos County also notified the U.S. Department of Health and Human Services.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4773.

Very truly yours,

M. Alexandra Belton of
MULLEN COUGHLIN LLC

MABB/kzs
Enclosure

EXHIBIT A

0000031

Coos County Family Health Services
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS1619

1_0000031 ###

[redacted]

October 9, 2025

Dear [redacted]:

Coos County Family Health Services ("Coos County") is writing to make you aware of a recent incident that may impact the information you have on file with us. This letter provides information about the incident, what we have done in response, and resources available to assist you in protecting your information, should you feel it is appropriate to do so.

What Happened? We became aware of suspicious activity related to our phone systems and computer servers. We began an investigation to determine the nature and scope of the activity and took steps to secure our systems. The investigation determined that there was unauthorized access to the servers on July 9, 2025, during which an unauthorized party may have viewed or copied data. In an abundance of caution, Coos County reviewed the files that may have been impacted and, on August 12, 2025, confirmed they contained patient information. We then worked to reconcile the individual records and determine contact information for patients, and we are now notifying individuals whose data was potentially in those files.

What Information Was Involved? The types of data that may have been present in the relevant files vary upon circumstances, but may have included a combination of certain individuals' names, dates of birth, contact information, Social Security numbers, medical identification numbers, and medical information.

What We Are Doing. We take this event and the security of personal information in our care very seriously. In response to this incident, we moved quickly to investigate and notify potentially affected individuals. As part of our ongoing commitment to the security of information, we are reviewing and enhancing our existing policies and procedures. As an added precaution, we are providing you with access to [redacted] months of free credit monitoring and identity protection services provided by TransUnion. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take To Help Protect Personal Information*. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements, medical claims, 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* where you will find more information on the credit monitoring and identity restoration services we are making available to you.

For More Information. If you have additional questions, or need assistance, please call the help line at [redacted]. Representatives are available for 90 days from the date of this letter to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. You may also write to us at 133 Pleasant Street, Berlin, NH 03570 or call 603-752-2040.

Sincerely,

Coos County Family Health Services

0000031

Steps You Can Take To Help Protect Personal Information

Enroll in Monitoring Services

In response to the 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 [redacted] months 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: [redacted] 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.

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/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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) 442-9828; 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 are approximately 60 Rhode Island residents that may be impacted by this event.