

Richard Halm
T (312)985-5564
F (312)985-5952
Email: rhalm@clarkhill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

July 20, 2026

VIA PORTAL

Nebraska Attorney General
2115 State Capitol
Lincoln, NE 68509

Dear Attorney General Hilgers,

We represent Penobscot Valley Hospital (“PVH”) with respect to a data security incident involving personal information as described below. PVH takes the security of the information in its control seriously and is committed to answering any questions you may have regarding this event.

1. Nature of security incident

On January 28, 2026, PVH was alerted to suspicious activity within its network. PVH immediately implemented its incident response procedures, took steps to secure systems, and hired third-party forensic specialists to assist with an investigation. On February 12, 2026, this investigation determined that certain files and folders may have been accessed by an unauthorized individual. PVH conducted a thorough review of the files at issue, and on June 4, 2026, the investigation determined that personal information may have been in the files impacted by this incident. Since then, PVH has been identifying missing addresses in order to effectuate the mailing.

Impacted information varied by individual but could have included names and one or more of the following: address, date of birth, Social Security number, medical information, and/or financial information.

2. Number of residents affected

5 Nebraska residents were former patients and were notified of the incident under HIPAA. Potentially impacted individuals were notified beginning July 20, 2026. A copy of the form notification letter is enclosed as Exhibit A.

3. Steps taken in response to the incident

In response to the incident, PVH has restored its systems, tightened access controls, and implemented additional technical safeguards to strengthen the security of their systems, among other measures. Additionally, letters were mailed to potentially affected individuals, which included instructions for enrolling in twelve (12) months of credit monitoring and identity protection services through TransUnion at no cost.

4. Contact information

July 20, 2026
Page 2

PVH takes the security of the information in its control seriously. If you have any questions or need additional information, please do not hesitate to contact me at rhalm@clarkhill.com or (312) 985-5564.

Sincerely,

CLARK HILL

A handwritten signature in dark ink that reads "Richard Halm". The signature is written in a cursive style with a small dot at the end.

Richard Halm
Member

cc: Lauren M. Williams – lmwilliams@clarkhill.com

PENOBSCOT VALLEY HOSPITAL
C/O CYBERSCOUT
P.O. Box 3826
Suwanee, GA 30024



174 1 33939 *****AUTO**5-DIGIT 04497



July 20, 2026

Notice of Data Security Incident

Dear [REDACTED]

Penobscot Valley Hospital experienced a data security incident that may have involved your protected health information (“PHI”). We take the privacy and security of your information seriously and sincerely apologize for any concern or inconvenience this incident may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What Happened?

On January 28, 2026, we were alerted to suspicious activity involving our information technology environment. In response, we initiated an investigation, took steps to secure our systems, and notified law enforcement. Additionally, a third-party forensic firm was engaged to assist in the investigation. On February 12, 2026, this investigation determined that an unauthorized individual may have accessed certain files and folders. On June 4, 2026, the investigation determined that your information may have been in the files impacted by this incident.

What Information Was Involved?

The information that may have been impacted includes your name and some combination of the following: address, date of birth, Social Security number, medical information related to your visit at Penobscot Valley Hospital, and/or financial information.

What We Are Doing:

To help prevent something like this from happening again, we have implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor our systems. Additionally, we are offering identity theft protection services through TransUnion.

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 twelve (12) 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.

How do I enroll in the free 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.

What You Can Do:

We recommend you review any financial statements and bills and explanation of benefits you may receive from your healthcare providers and health insurance plans. If you notice any services that were not received, but are on the bills explanation of benefits, please contact the provider or health plan immediately.

Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information:

If you have any questions or concerns, please call 1 833-319-8871 Monday through Friday from 9 am - 9 pm Eastern Time. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Penobscot Valley Hospital

Recommended Steps to Help Protect Your Information

1. Website and Enrollment.

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] 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.

2. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

3. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

4. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia Residents: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, Iowa 50319; 515-281-5926; consumer@ag.iowa.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your 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.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. A total of 91 Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.