March 6, 2026

Martin McElligott
312.821.6219 (direct)
Martin.McElligott@wilsonelser.com

Via Online Portal:

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capitol
Lincoln, NE 68509

Re: Notice of Cybersecurity Incident Involving Cedar Valley Hospice

Dear Attorney General Hilgers:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents the Cedar Valley Hospice ("Cedar Valley") (900 Tower Park Drive, Waterloo, IA 50701). The purpose of this correspondence is to provide your office with notice of a cybersecurity incident that was first discovered by Cedar Valley on November 11, 2025, (hereinafter, the "Incident"). Cedar Valley takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Nebraska residents being notified, and the steps that Cedar Valley has taken in response to the Incident. We have also attached a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring and identity theft protection services.

1. Nature of the Incident

On November 11, 2025, Cedar Valley detected suspicious activity on their network that resulted in a network interruption. Cedar Valley immediately isolated the impacted environment and worked with its IT professionals and outside experts to secure and remediate the server. Cedar Valley engaged a third-party cybersecurity firm to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The investigation determined that an unauthorized third-party potentially viewed and/or downloaded data stored on certain of Cedar Valley's systems.

Based on these findings, Cedar Valley conducted an extensive review of the impacted data files to identify the specific individuals and the types of information that may have been compromised. On February 23, 2026, Cedar Valley finalized the list of individuals to notify. The type of information that may have been compromised includes individuals' names, Social Security numbers, driver's license information, and financial account information. At this time, Cedar Valley is not aware of any misuse of anyone's personal information and has not received any reports of fraud or identity theft related to this Incident.

2. Number of Nebraska residents affected.

A total of one (1) Nebraska resident may have been potentially affected by this Incident. The notification letter to this individual was mailed on March 4, 2026, by U.S. mail. A sample (redacted) copy of the notification letter is included with this letter as **Exhibit A**.

3. Steps taken in response to the Incident.

Data privacy and security is among one of Cedar Valley's highest priorities, and Cedar Valley is committed to doing everything it can to protect the privacy and security of the personal information in its care. Since the discovery of the Incident, Cedar Valley worked with IT professionals and outside experts to secure and remediate their network environment. Cedar Valley engaged a third-party cybersecurity firm to conduct a comprehensive forensic investigation to determine the nature and scope of the Incident. Furthermore, Cedar Valley is implementing additional technical safeguards, enhanced security measures, and updated policies and procedures to mitigate against the risk of future issues.

Cedar Valley has also offered all impacted individuals with complimentary credit monitoring and identity theft protection services by Kroll for a period of twelve (12) months. In addition, Cedar Valley has highlighted steps that individuals can take to protect themselves including actively monitoring their financial accounts and statements, requesting a free credit report, and placing a fraud alert or security freeze on their credit reports.

4. Contact information

Cedar Valley remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact the undersigned at Martin McElligott@WilsonElser.com or 312-821-6219.

Very truly yours,

WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

Martin McElligott

EXHIBIT A

CEDAR VALLEY HOSPICE®

[redacted]

[redacted]

KROLL

SCAN TO ENROLL

<<Date>> (Format: Month Day, Year)

Re: Notice of Data Breach

Dear [redacted],

Cedar Valley Hospice is writing to inform you of a recent data incident that may have resulted in unauthorized access to your personal information<<b2b_text_2(provided to us to obtain or carry out case management services on your behalf)>>. While we are unaware of any fraudulent use of your personal information at this time, we are providing you with details about the Incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On November 11, 2025, Cedar Valley Hospice detected suspicious activity on our network that resulted in a network interruption. We promptly initiated an investigation with the assistance of a third-party cybersecurity firm to determine the nature and scope of the incident.

What Information Was Involved?

On November 19, 2025, the investigation determined that learned that an unauthorized third-party potentially viewed and/or downloaded data stored on certain of Cedar Valley Hospice's systems. Based on the investigation, we began a comprehensive review of the impacted data set to determine what sensitive and/or personal information was impacted and to whom it related. On December 30, 2025, we completed our review and confirmed that your personal information was contained in the impacted data. More specifically, the impacted systems potentially contained your [redacted].

What We Are Doing

Data privacy and security is among our highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Since the discovery of the incident, we have taken additional steps to reduce the risk of this type of incident occurring in the future by enhancing our technical security measures and procedures.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<ServiceTerminMonths>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until [redacted] *to activate your identity monitoring services.*

Membership Number: [redacted]

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What You Can Do

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, 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 questions, please call (844) 443-1312, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction. We sincerely regrets any concern or inconvenience this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Cedar Valley Hospice

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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 should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit-report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.