McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

Colin M. Battersby
Direct Dial: (248) 593-2952
E-mail: cbattersby@mcdonaldhopkins.com

October 7, 2025

VIA U.S. MAIL:
Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Sierra Vista Hospital & Clinics – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Sierra Vista Hospital & Clinics ("Sierra Vista"). Truth or Consequences, New Mexico,[1] Sierra Vista is a hospital. I am writing to provide notification of an incident at Sierra Vista that may affect the security of personal information of approximately four (4) New Hampshire residents. By providing this notice, Sierra Vista does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction. Notice is being provided under the Health Insurance Portability and Accountability Act Breach Notification Rule, 45 C.F.R. §§ 164.400-414 ("HIPAA" or "Final Rule").

On or about January 29, 2025, Sierra Vista detected unauthorized access to their network. Upon learning of the issue, Sierra Vista commenced a prompt and thorough investigation. As part of our investigation, Sierra Vista has worked very closely with external data privacy professionals experienced in handling these types of incidents. Sierra Vista's review concluded recently and discovered on August 13, 2025, that between January 14, 2025 and January 31, 2025, protected health information was included within the data that may have been viewed or acquired by the unauthorized actor. The potentially impacted data elements include full name and SSN.[2]

Sierra Vista is not aware of any reports of identity fraud or improper use of the information as a direct result of this incident. Nevertheless, out of an abundance of caution, Sierra Vista wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Siera Vista is providing the affected residents with written notification of this incident commencing on or about October 6, 2025 in substantially the same form as the letter attached hereto. Sierra Vista is also offering residents who had a Social Security number impacted with complimentary one-year membership for credit monitoring services. Sierra Vista is advising the affected residents to always remain vigilant in

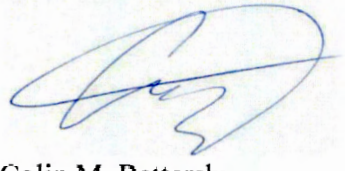
[1] 800 E. 9th Avenue Truth or Consequences, NM 87901
[2] Of the 4 individuals in New Hampshire notified only two (2) individuals had potentially impacted data elements which would trigger notifications under New Hampshire law. All four (4) individuals had data elements potentially impacted which would not trigger notifications under New Hampshire law.

reviewing financial account statements for fraudulent or irregular activity on a regular basis. Sierra Vista is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit file and obtaining a free credit report. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Sierra Vista, protecting the privacy of personal information is a top priority. Sierra Vista is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Sierra Vista continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com.

Very truly yours,



Colin M. Battersby

Encl.

Exhibit A

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

[redacted]

[redacted]

[redacted]

Dear [redacted]

The privacy and security of the personal information we maintain is of the utmost importance to Sierra Vista Hospital & Clinics ("Sierra Vista"). We are writing to provide you with information regarding a recent cybersecurity incident that potentially involved your personal information. Please read this notice carefully, as it provides information about the incident, the complimentary identity monitoring services we are making available to you, and the significant measures we take to protect your information.

What Happened?
On or about January 29, 2025, Sierra Vista detected unauthorized access to our network as a result of a cybersecurity incident that resulted in the exposure of certain data we maintain.

What We Are Doing.
Upon learning of the issue, we secured our network and commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Following the completion of our investigation, it was determined that some of our files may have been accessed or removed by the unauthorized individual(s) between January 14, 2025 and January 31, 2025. We conducted a thorough review of the potentially impacted data and on August 13, 2025, we determined that the impacted files may have contained your personal and/or protected health information.

While cybersecurity threats continue to impact all of us, we are taking ever-increasing measures to protect the information entrusted to us. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. In response to this incident and through our continuing comprehensive review, we have strengthened our network and implemented additional security improvements recommended by third-party cyber security experts. We have increased email filtering, added additional malware monitoring, and added additional cybersecurity training for our employees.

What Information Was Involved?

The information that may have been accessed contained your [redacted]

What You Can Do.

To date, we do not have evidence that your information has been used to commit financial fraud or identity theft. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and provide you access to complimentary credit monitoring services through Experian IdentityWorks[SM] for [redacted] as a precaution. This letter provides more information about the complimentary services, enrollment instructions, and other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. To the extent it is helpful, we have also provided information on protecting your medical information on the following pages.

For More Information.

If you have questions, please contact our dedicated and confidential call center at 855-291-2594. The response line is available for 90 days from the date of this letter, between the hours of 9:00 a.m. – 9:00 p.m. Eastern time, Monday through Friday, excluding holidays. We apologize for any inconvenience or concern this may cause. We have taken this matter very seriously and will continue to take significant measures to protect the personal information in our possession.

Sincerely,

Sierra Vista Hospitals & Clinics
800 E. 9th Avenue
Truth or Consequences, New Mexico 87901

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for [redacted]. Please note that Identity Restoration is available to you for [redacted] 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 [redacted] 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:

- Ensure that you **enroll by** [redacted] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: [redacted]

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 (877) 288-8057 by [redacted] Be prepared to provide engagement number [redacted] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 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.

2. Placing a Fraud Alert.

We recommend that you place a one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(888) 378-4329; (800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
www.transunion.com/fraud-alerts
(800) 916-8800; (800) 680-7289

** 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.

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	*Experian Security Freeze*	*TransUnion Security Freeze*
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348-5788	Allen, TX 75013	Woodlyn, PA 19094
www.equifax.com/personal/credit-report-services/credit-freeze/	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze
(888) 298-0045; (800) 685-1111	(888) 397-3742	(800) 916-8800; (888) 909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as copy of a government issued identification. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. If you do place a security freeze prior to enrolling in a credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Protecting Your Medical Information.

If this notice letter indicates that your medical information was impacted, we have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. The following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

6. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

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. In addition, you have the right to obtain a security freeze (as explained above) or submit a declaration of removal. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act. For more information about the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: 877-877-9392.

Rhode Island Residents: You have the right to obtain a police report if one was filed, or alternatively, you can file a police report. Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. There were <<RI Count>> of Rhode Island residents impacted.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, oag.dc.gov/consumer-protection, Telephone: 202-442-9828.