RECEIVED

MAR 18 2024

CONSUMER PROTECTION

WILSON ELSER

March 12, 2024

Via U.S. Mail
Attorney General John Formella
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Re:	Our Client	:	Hendry Regional Medical Center
	Matter	:	Data Security Incident on August 25, 2022
	Wilson Elser File #	:	15991.01313

Dear Attorney General Thomas Donovan Jr.:

We represent Hendry Regional Medical Center ("HRMC") located in Clewiston, Florida with respect to a potential data security incident described in more detail below. HRMC takes the security and privacy of the information in its control 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 security breach, the number of New Hampshire residents that were potentially affected, what information has been compromised, and the steps that HRMC is taking to secure the integrity of its systems. We have also enclosed hereto samples of the notifications made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On August 25, 2022, HRMC detected that it was a target of a cybersecurity incident, whereby an unauthorized third party gained temporary access to HRMC's computer network. This incident may have resulted in the exposure of personal information. Upon detecting this incident, HRMC moved quickly to secure their network environment and launched a thorough investigation. The investigation was performed with the help of external IT specialists to determine the scope and extent of the potential unauthorized access to their systems and any personal information. Although we have found no evidence that any information has been specifically accessed for misuse, it is possible that the potentially impacted individuals'

could have been exposed as a result of this attack.

294109507v.1
294109507v.1

As of this writing, HRMC has not received any reports of related identity theft since the date of the incident (August 25, 2022, to present).

2. Number of New Hampshire Resident(s) Notified.

A total of ten (10) residents of New Hampshire were potentially affected by this security incident. These individuals are current and former patients of HRMC. A notification letter to these individuals will be mailed on March 12, 2024, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Immediately upon learning of this incident, HRMC moved quickly to secure its network, and contacted a reputable third-party forensic team to assist with its investigation. Since then, HRMC has been working with law enforcement to help respond to this incident, along with cybersecurity experts to review all policies and procedures relating to the security of HRMC's systems. This forensic investigation, which concluded on September 22, 2022, identified evidence to suggest that a limited amount of data from our servers was accessed during the incident. Some of the data in question relates to information held on current and former patients and employees. Based on these findings, HRMC performed data mining on the affected systems to identify the specific individuals and the types of information that may have been compromised. On December 5, 2022 we were able to notify an initial wave of impacted individuals. HRMC proceeded with substitute notice pursuant to HIPAA on February 23, 2023. Since that time, we have identified additional individuals who will be notified.

Although HRMC is not aware of any evidence of misuse of personal information, HRMC extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through Cyberscout. This service will include of credit monitoring, along with a fully managed identity theft recovery service, should the need arise.

4. Contact Information

HRMC 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 me at

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Joseph M Fusz

Copy: Anjali Das, Esq. (Wilson Elser, LLP)
Shaun G. Goodfriend, Esq. (Wilson Elser, LLP

Enclosures: *Sample Notification Letter*

Hendry Regional Medical Center
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

HENDRY REGIONAL MEDICAL CENTER
"Where It's All About Getting Better"

March 12, 2024

Via First-Class Mail

Notice of Data Security Incident

Dear FIRST LAST,

Hendry County Hospital Authority d/b/a Hendry Regional Medical Center ("HRMC") is a 25-bed critical access hospital located in Clewiston, Florida. We are writing to inform you of an incident that may have exposed your personal information to unauthorized parties. We take data security incidents like this very seriously and want to provide you with information and resources you can use to protect your information moving forward.

What Happened?

On August 25, 2022, HRMC detected that it was the target of a cybersecurity incident, whereby an unauthorized third party gained temporary access to HRMC's computer network. Upon detecting this incident, we moved quickly to secure our network environment and launched a thorough investigation. The investigation was performed with the help of external IT specialists to determine the scope and extent of the potential unauthorized access to our systems and any personal information.

This forensic investigation, identified evidence to suggest that a limited amount of data from our servers was accessed during the incident. Some of the data in question relates to information held on current and former patients. Based on these findings, HRMC performed data mining on the affected systems to identify the specific individuals and the types of information that may have been compromised. Due to the complex nature of the data involved, HRMC proceeded with substitute notice which has been available on our website since February, 2023.

What Information was Involved?

Based on the investigation, the following information related to you may have been subject to unauthorized access: . Please note that not all information was potentially impacted for each individual.

We take our data responsibilities and protection of your data very seriously and we are sorry for any worry and inconvenience this news will cause. As of this writing, we have not received any reports of related identity theft since the date of the incident (August 25, 2022 to present). We would like to reassure you that we have taken all efforts possible to mitigate any further exposure of your personal information and we are committed to supporting you.

What We Are Doing.

Data privacy and security is among HRMC's 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, HRMC moved quickly to investigate, respond, and confirm the security of our systems. Specifically, HRMC has taken and are continuing to take steps to prevent a similar event from occurring in the future by implementing additional safeguards and enhanced security measures to better protect the privacy and security of information in our systems, which includes, but is not limited to, changing all passwords and updating our firewall and VPN. We have also reviewed and taken steps to enhance our policies and procedures relating to the security of our systems and servers, as well as our information life cycle management.

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 the 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 **www.mytrueidentity.com** and follow the instructions provided. When prompted please provide the following unique code to receive services: **(CODE).** 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 encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

For More Information

If you have any questions or concerns not addressed in this letter, we encourage you to contact Cyberscout with any questions and enroll in free services by calling 1-833-510-0375. Cyberscout is available 8:00 am to 8:00 pm ET, Monday through Friday, excluding holidays.

Again, we encourage you to take full advantage of this service offering. Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Hendry Regional Medical Center values the security of your personal data, and we apologize for any inconvenience this incident has caused.

Sincerely,

R.D. Williams
Chief Executive Officer,
Hendry Regional Medical Center

*Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

File Police Report: You have the right to file or obtain a police report if you 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade

Commission, or your state Attorney General. The Federal Trade Commission can be reached 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. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed 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.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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 violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at 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 residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of *Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island:* You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

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

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov