

May 5, 2023

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

CONFIDENTIAL

Via Email Only

Attorney General Brian Frosh

Office of the Attorney General

Attn: Security Breach Notification

200 St. Paul Place

Baltimore, MD 21202

IDTheft@oag.state.md.us

Re: Cybersecurity Incident Involving Maryland Health Systems d/b/a Lorien Health Services

Dear Attorney General Frosh:

Our law firm, Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”), represents Maryland Health Systems d/b/a Lorien Health Services (“LHS”), a general health care services provider specializing in elderly and assisted living care, located at 3300 N Ridge Rd. #390, Ellicott City, Maryland 21043, with respect to a recent cybersecurity incident that was first discovered by LHS on March 23, 2023 (hereinafter, the “Incident”). LHS 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.

The purpose of this correspondence is to provide the Maryland Attorney General with preliminary notice of a cybersecurity incident involving LHS, while the investigation is ongoing. Once the investigation has been completed, we will submit a supplemental report with additional information regarding the impacted Maryland residents, if any.

1. Nature of the Incident

On March 23, 2023, LHS detected unusual activity on one of its business email accounts. Upon discovery of this incident, LHS immediately secured the account and promptly engaged a specialized third-party cybersecurity firm to conduct an investigation to determine the nature and scope of the incident. At this time, the forensic investigation is ongoing.

Although LHS is unaware of any fraudulent misuse of information and is still awaiting the results of the forensic investigation, it is possible (but not yet confirmed) that the email account in question may have contained patients’ name, data of birth, and medical diagnosis.

As of this writing, LHS has not received any reports of misuse of patient information or related identity theft since the date of the incident (March 23, 2023 to present).

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Los Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

2. Number of Maryland residents affected.

LHS is in the process of confirming whether any Maryland residents were affected by this Incident. LHS will be able to confirm which, if any, individuals were impacted after the completion of the forensic investigation and data mining of the account. LHS will provide prompt notice to individuals when the confirmed results of the forensic investigation are produced, in addition to providing the Maryland Attorney General with a supplemental report regarding the number of impacted Maryland residents

3. Steps taken in response to the Incident.

LHS is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, LHS moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, LHS engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, LHS changed the impacted email account credentials; upgraded multifactor authentication requirements, and took steps and will continue to take steps to mitigate the risk of future harm.

Although LHS is not aware of any actual or attempted misuse of the affected personal information, LHS intends to offer 12 months of complimentary credit monitoring and identity theft restoration services to any individual impacted by this incident to help protect their identity. Additionally, LHS will provide guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

LHS 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 Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

June 29, 2023

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

CONFIDENTIAL

Via Email Only

Attorney General Brian Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Re: Cybersecurity Incident Involving Maryland Health Enterprises d/b/a Lorien Health Services

Dear Attorney General Frosh:

Our law firm, Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”), represents Maryland Health Enterprises d/b/a Lorien Health Services (“LHS”), with respect to a recent cybersecurity incident (hereinafter, the “Incident”). Pursuant to MD Comm L Code § 14-3504 (2017), we write to supplement our previous report dated May 5, 2023 to further inform you of the Incident, what information may have been compromised, and the steps that LHS has taken in response to the Incident.

1. Nature of the Incident

On March 23, 2023, LHS detected unusual activity on one of its business email accounts. Upon discovery of this incident, LHS immediately secured the account and promptly engaged a specialized third-party cybersecurity firm to conduct an investigation to determine the nature and scope of the incident. The investigation was completed on May 10, 2023, and the list of impacted individuals was finalized on May 30, 2023.

Although LHS is unaware of any fraudulent misuse of information, the forensic investigation determined that the email account in question may have contained persons’ name, health information, medication information, and medical insurance information. The health information impacted is believed to be from an invoice only. Please be assured that the impacted information was very limited, and no lab or test results were disclosed.

As of this writing, LHS has not received any reports of misuse of patient information or related identity theft since the date of the incident (March 23, 2023 to present).

2. Number of Maryland residents affected.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

A total number of 129 Maryland residents may have been potentially affected by this incident. Notification letters to these individuals will be mailed on June 29, 2023, by first class mail. A sample copy of the notification letter is included with this letter under *Exhibit A*.

3. Steps taken in response to the Incident.

LHS is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, LHS moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, LHS engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, LHS changed the impacted email account credentials; upgraded multifactor authentication requirements, and took steps and will continue to take steps to mitigate the risk of future harm.

Although LHS is not aware of any actual or attempted misuse of the affected personal information, LHS intends to offer 12 months of complimentary credit monitoring and identity theft restoration services to any individual impacted by this incident to help protect their identity. Additionally, LHS will provide guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

LHS 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 Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

Maryland Health Enterprises
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-07602



[REDACTED]
[REDACTED]
[REDACTED]

June 29, 2023

Via First-Class Mail

Dear [REDACTED],

Maryland Health Enterprises d/b/a Lorien Health Services ("LHS") is writing to inform you of a recent data security incident that may have resulted in an unauthorized access to your sensitive personal information. 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. Please be assured LHS takes the protection and proper use of your personal information very seriously.

What Happened?

On March 23, 2023, LHS detected unusual activity on one of its business email accounts resulting from an attempt to manipulate fictitious payments. Upon discovery of this incident, LHS immediately secured the account and promptly engaged a specialized third-party cybersecurity firm to conduct an investigation to determine the nature and scope of the incident. The investigation was completed on May 10, 2023, and the list of impacted individuals was finalized on May 30, 2023.

What Information was Involved?

Although LHS is unaware of any fraudulent misuse of information, the forensic investigation determined that the email account in question may have contained patients' name, health information, medication information, and medical insurance information. The health information impacted is believed to be from an invoice only. Please be assured that the impacted information was very limited, and no lab or test results were disclosed.

As of this writing, LHS has not received any reports of misuse of patient information or related identity theft since the date of the incident (March 23, 2023 to present).

What We Are Doing.

We take the security of all information in our control very seriously. Given this, we have 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. 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.

What You Can Do.

In response to the incident, we are also 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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to **<https://secure.identityforce.com/benefit/lorienhealth>** 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.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call 1-800-405-6108 Monday through Friday, during the hours of 8:00 am to 8:00 pm Eastern Time (excluding U.S. national holidays). Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

LHS values the security of your personal data, and we apologize for any inconvenience that this incident has caused.

Sincerely,



Karen Cole, PT, CHC, RAC-CT, RAC-CTA
Lorien Health Services
Corporate Compliance and Privacy Officer

Steps You Can Take Help Protection 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.

Security Freeze: You also 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:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.h tml	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze
---	--	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

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. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

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. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of

known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Arizona residents, the Attorney General may be contacted at the Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025.

For Colorado residents, the Attorney General may be contacted through Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000, www.coag.gov.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Illinois residents, the Attorney General can be contacted at 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov.

For Iowa residents, you can report any suspected identity theft to law enforcement or to the Attorney General.

For Massachusetts residents, 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 Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also 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 New York residents, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>.

For Oregon residents, state law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For Rhode Island residents, this incident involves 0 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).