MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

April 5, 2022

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent NHS Management, LLC ("NHS") located at 931 Fairfax Park, Tuscaloosa, AL 35406 and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. This notice may be supplemented with new significant facts learned subsequent to its submission. By providing this notice, NHS does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On May 16, 2021, NHS discovered that it was the victim of a sophisticated cyberattack. NHS immediately launched an investigation to confirm the full nature and scope of the incident and restore functionality to impacted systems. Through the investigation, NHS determined that an unauthorized actor accessed certain NHS systems between February 25, 2021 and May 16, 2021. Although there is no evidence of any identity theft or fraud in connection with this incident, the accessible and potentially accessible documents from these systems were reviewed to determine what, if any, personal information was contained within them. On June 16, 2021, the investigation identified that information of 14 individuals was impacted by the event. NHS provided notice to these 14 individuals on July 4, 2021. An extensive review to identify additional personal information that may be impacted by the event remained ongoing until February 4, 2022. On February 4, 2022, the extensive review identified additional personal information was present within the accessed documents. NHS then undertook efforts to confirm the identities of the individuals whose information was present in the affected documents and began providing notice once it had located the contact information to do so. The information that could have been subject to unauthorized access includes name and Social Security number.

Notice to New Hampshire Resident

On or about April 5, 2022, NHS provided written notice of this incident to affected individuals, which includes approximately one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, NHS moved quickly to investigate and respond to the incident, assessed and increased the security of relevant NHS systems, and notify potentially affected individuals. Additionally, NHS notified and cooperated with federal law enforcement, as well as appropriate federal agencies. NHS is also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event. NHS is providing access to credit monitoring services for one (1) year, through Kroll, to individuals whose personal information including Social Security numbers was potentially affected by this incident, at no cost to these individuals.

Additionally, NHS is providing impacted individuals with guidance on how to better protect against identity theft and fraud. NHS is providing individuals with 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

Rebecca Jones

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/nad
Enclosure

EXHIBIT A

NHS MANAGEMENT, L.L.C.

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_3(NOTICE OF)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

At NHS Management, LLC ("NHS") we take the privacy and security of personal information seriously. Thus, we are writing to inform you of an incident that may affect the security of some of your personal information. NHS provides consulting services to nursing and physical rehabilitation facilities located in Alabama, Arkansas, Florida, Missouri, a list of which can be found at the end of this letter. NHS Management collects personal information related to our employees and vendors, as well as the patients/residents of the facilities we serve and the family members and guardians of such patients and residents. While we are unaware of any actual misuse of your information, we want to provide you with information about the incident, our response, and resources available to help protect your information from possible misuse, should you wish to do so.

What Happened? On May 16, 2021, NHS discovered that it was the victim of a sophisticated cyberattack. NHS immediately took steps to stop the attack and mitigate the harm. NHS launched an investigation with the assistance of a third-party forensic team to confirm the full nature and scope of the incident and restore functionality to impacted systems. Through our investigation, we determined that an unauthorized actor accessed certain NHS systems and information stored therein between February 25, 2021 and May 16, 2021. Although we have no evidence of any identity theft or fraud in connection with this incident, the documents located on these systems that were determined to have been accessed or potentially accessible were reviewed by a third-party data review team to determine what, if any, personal information was contained within them. On February 4, 2022, this extensive review identified certain personal information was present within the affected documents. NHS then undertook efforts to confirm the identities of the individuals whose information was present in the documents and began providing notice once we located the contact information to do so.

What Information Was Involved? Our investigation determined that some of your information was accessible by an unknown actor as a result of this incident. This information includes your name and <<b2b_text_1(data elements)>> <<b2b_text_2(data elements cont.)>>. Please note that, to date, we are unaware of any actual or attempted misuse of your information as a result of this incident.

What We Are Doing. Upon learning of this incident, we moved quickly to investigate and to assess and increase the security of relevant NHS systems. We also notified and cooperated with federal law enforcement, as well as appropriate federal agencies. As part of our ongoing commitment to the security of information, we are also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

We are offering you access to complimentary identity monitoring services for 12 months through Kroll. These services include credit monitoring, fraud consultation and identity theft restoration. If you wish to activate the identity monitoring services, you may follow the instructions included in the *Steps You Can Take to Help Protect Your Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits, and credit reports for suspicious activity and to detect errors over the next 12 to 24 months. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Information.* There you will also find more information on the identity monitoring services we are making available to you. While NHS will cover the cost of these services, you will need to complete the activation process, as we cannot activate the services on your behalf.

For More Information. If you have additional questions regarding this incident, please call our dedicated assistance line at 1-???-???-???? between the hours of 8:00 a.m. and 5:30 p.m. Central Time, Monday – Friday, excluding major U.S. holidays. You may also write to NHS at 931 Fairfax Park, Tuscaloosa, AL 35406.

We sincerely regret any inconvenience or concern this incident may have caused and are happy to answer any questions you may have.

Sincerely,

Anita Helms

Anita Helms
Corporate Compliance/Privacy Officer
https://www.nhsmanagement.com

List of facilities: Columbiana Health and Rehabilitation, LLC, Legacy Health and Rehab of Pleasant Grove, LLC, Oak Knoll Health and Rehabilitation, LLC, South Haven Health and Rehabilitation, LLC, Aspire Physical Recovery Center at Hoover, LLC, Civic Center Health and Rehabilitation, LLC, South Health and Rehabilitation, LLC, Aspire Physical Recovery Center at Cahaba River, LLC, Northway Health and Rehabilitation, LLC, Lineville Health and Rehabilitation, LLC, Fayetteville Health and Rehabilitation Center, Legacy Health and Rehabilitation Center, Paris Health and Rehabilitation Center, Springdale Health and Rehabilitation Center, Covington Court Health and Rehabilitation Center, Carthage Health and Rehabilitation Center, Joplin Health and Rehabilitation Center, Pleasant Hill Health and Rehabilitation Center, Warsaw Health and Rehab Center, Webb City Health and Rehabilitation Center, Cordova Health and Rehabilitation, LLC, Crossville Health and Rehabilitation, LLC, Hendrix Health and Rehabilitation, Jacksonville Health and Rehabilitation, LLC, Athens Health and Rehabilitation, LLC, Valley View Health and Rehabilitation, LLC, Huntsville Health and Rehabilitation, LLC, Crystal River Health and Rehabilitation Center, Daytona Beach Health and Rehab Center, Ocala Health and Rehabilitation Center, St. Augustine Health and Rehabilitation Center, West Melbourne Health and Rehabilitation Center, Florala Health and Rehabilitation, LLC, Luverne Health and Rehabilitation, LLC, Opp Health and Rehabilitation, LLC, Ozark Health and Rehabilitation, LLC, Tallassee Health and Rehabilitation, LLC, Wetumpka Health and Rehabilitation, LLC, Aspire Physical Recovery Center at West AL, LLC, Glen Haven Health and Rehabilitation, LLC, Hunter Creek Health and Rehabilitation, LLC, Martin Glen , LLC d/b/a Martinview (SCALF) & Martinview W (ALF), Moundville Health and Rehabilitation, LLC, Park Manor Health and Rehabilitation, LLC, Sumter Health and Rehabilitation, LLC, Georgiana Health and Rehabilitation, LLC, Ashland Place Health and Rehabilitation, LLC, Gulf Coast Health and Rehabilitation, LLC, Palm Gardens Health and Rehabilitation, LLC, Prattville Health and Rehabilitation, LLC.

Steps You Can Take to Help Protect Your Information

Activate Your Identity Monitoring Services:

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. To activate these services, please see the below instructions:

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

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

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

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);

2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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 and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For 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 bureaus 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 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. We encourage you to 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.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 33 Rhode Island residents impacted by this incident.