Notice of Data Privacy Event

NHS Management, LLC ("NHS") is providing notice of a data event that may affect the security of certain information. When NHS became aware of suspicious activity related to certain of its systems, with the assistance of third-party computer forensic specialists, we took immediate steps to contain the incident and to investigate the nature and scope of the incident. NHS is issuing this notice to provide additional details regarding what is known about the incident, the steps we are taking in response, and steps those who may be impacted by this event can take if they wish to do so.

What Happened? 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 our investigation, we determined that an unauthorized actor may have had access to certain NHS systems between May 14, 2021 and May 16, 2021. As a result of the investigation, it was determined that certain files were potentially at risk as the result of the incident. It was determined that these additional files required further review. Due to the volume and complexity of the files at issue, NHS promptly began working with a third-party data review team to perform a comprehensive review of all information contained in the impacted files. At present, the comprehensive data review is still ongoing in an effort to determine what personal information may have been contained within same. Out of an abundance of caution, NHS is providing this notice to its employees as well as nursing home facility residents and patients because personal information was contained within the affected systems and may have been accessed. Our efforts to identify potentially impacted individuals and contact information to directly notify those potentially impacted individuals are ongoing. Any impacted individuals identified thus far have already been notified.

What Information Was Involved? The information that may have been impacted by this incident could have included one or more of the following: an individuals' name; address and other contact information; medical history; treatment or diagnosis information; health information; health insurance information; Social Security number, date of birth, and/or driver's license number. However, not every data element would have been impacted for every individual, and there is no evidence of unauthorized access to the database that contains electronic medical records. **Please note that we are unaware of any actual or attempted misuse of any information as a result of this incident.**

How Will Individuals Know If They Are Affected? We are currently in the process of an extensive review of the impacted systems to identify the individuals whose information was stored on those systems and could have been subject to unauthorized access. We will provide written notification to the individuals for whom we have valid mailing addresses, as soon as practicable after those individuals are identified.

What We Are Doing. Upon learning of this incident, we moved quickly to investigate, to assess and increase the security of relevant NHS systems, and to identify and notify affected individuals. We also notified the U.S. Department of Health & Human Services' Office for Civil Rights and federal law enforcement. 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.

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. You may also review the information in the *Steps You Can Take to Help Protect Your Information*, provided below.

For More Information. For more information you may contact NHS at 833-477-0672 between the hours of 8:00 a.m. and 5:00 p.m. Monday – Friday, Central Time. You may also write to NHS at 931 Fairfax Park, Tuscaloosa, AL 35406.

Steps You Can Take to Help Protect Your Information

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.