



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Vincent F. Regan
Office: (267) 930-4842
Fax: (267) 930-4771
Email: vregan@mullen.law

309 Fellowship Road, Suite 200
Mt. Laurel, NJ 08054

November 21, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Hope Health Systems Inc. (“HHS”) located at 1726 Whitehead Road, Suite 106, Gwynn Oak, Maryland 21207, and are writing to notify your office of an incident that may affect the security of certain personal information relating to nine thousand three hundred forty-one (9,341) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, HHS does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On June 20, 2022, HHS discovered encrypted files on certain computer systems. They immediately launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the incident. The investigation determined that there was unauthorized access to certain HHS servers beginning on June 10, 2022. On or about August 24, 2022, HHS determined it was unable to rule out unauthorized access to data stored on its affected systems. The investigation found no evidence that specific information was actually viewed by an unauthorized individual, but the investigation was unable to rule this activity out with absolute certainty. As access to data stored within their system could not be ruled out, they immediately undertook a review of the data at issue. This process completed on or about October 18, 2022. Out of an abundance of caution, HHS is providing notice to the individuals identified. HHS has seen no evidence of misuse of any information related to this incident.

The information associated with Maryland residents that could have been subject to unauthorized access includes name, Social Security number, date of birth, Driver's License number, medical information, and health insurance information.

Notice to Maryland Residents

On or about November 21, 2022, HHS provided written notice of this incident to nine thousand three hundred forty-one (9,341) Maryland residents. 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, HHS moved quickly to investigate and respond to the incident, assess the security of HHS systems, and identify potentially affected individuals. Further, HHS reported this incident to law enforcement, and they are taking steps to implement additional safeguards and review policies and procedures relating to data privacy and security. HHS is providing access to credit monitoring services for 12 months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, HHS is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. HHS is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

HHS is providing written notice of this incident to relevant state and federal regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4842.

Very truly yours,

Vincent F. Regan of
MULLEN COUGHLIN LLC

VFR/kml
Enclosure

EXHIBIT A



P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-896-4932
Or Visit:
<https://response.idx.us/hhs/>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

November 21, 2022

RE: Notice of Data <<Variable Data 1>>

Dear <<First Name>> <<Last Name>>:

Hope Health Systems, Inc. ("HHS") is writing to notify you of a recent data security event that may impact the privacy of some of your information. Although we are currently unaware of any misuse of your information, we are providing you with information about the incident and steps you may take to protect against misuse of your information, should you feel it necessary to do so.

What Happened? On June 20, 2022, HHS discovered encrypted files on certain computer systems. We immediately launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the incident. Our investigation determined that there was unauthorized access to certain HHS servers beginning on June 10, 2022. On or about August 24, 2022, HHS determined it was unable to rule out unauthorized access to data stored on its affected systems. The investigation found no evidence that your specific information was actually viewed by an unauthorized individual, but our investigation was unable to rule this activity out with absolute certainty. Once we made the determination that we could not rule out access to data stored within our system, we immediately undertook a review of the data at issue, and on October 18, 2022, we determined that certain data relating to you was included in the affected servers. Out of an abundance of caution, we are providing notice to you. HHS has seen no evidence of misuse of any information related to this incident.

What Information Was Involved? The data that relates to you and may have been affected by this incident includes your name, <<Data Elements>>.

What We Are Doing? Upon discovery, we immediately commenced an investigation to confirm the nature and scope of the incident. We reported this incident to law enforcement, and we are taking steps to implement additional safeguards and review policies and procedures relating to data privacy and security.

Although we are unaware of any actual or attempted fraudulent misuse of your information as a result of this incident, we are offering you access to <<12 months/24 months>> of complimentary credit monitoring through IDX. In addition, we are providing notice to appropriate regulatory authorities.

What You Can Do? We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits statements, and monitoring your free 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 instructions to enroll in the free credit monitoring and identity protection services we are making available to you. While HHS will cover the cost of these services, you will need to complete the activation process yourself, as we are unable to enroll you on your behalf.

For More Information. We regret any concern this incident may cause, and recognize that you may have questions that are not addressed in this letter. If you have additional questions or concerns, please call our toll-free dedicated assistance line at 1-833-896-4932. This toll-free line is available Monday – Friday from 9:00 am to 9:00 pm Eastern Time. Individuals may also write to Hope Health Systems, Inc., IT Director, 1726 Whitehead Road, Gwynn Oak, MD 21207.

Sincerely,

Executive Management
Hope Health Systems, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

1. Website and Enrollment. Go to <https://response.idx.us/hhs/> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline for enrollment is February 21, 2023.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-896-4932 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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 Massachusetts Residents, Under Massachusetts law, you have the right to obtain any 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 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. You may obtain information from these sources and/or the Federal Trade Commission using the contact information noted above about steps you can take to avoid identity theft. You may also write to HHS at 1726 Whitehead Road, Suite 106, Gwynn Oak, Maryland 21207.

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.