



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

NH DEPT OF JUSTICE
MAR 27 '23 PM 3:07

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

March 24, 2023

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

To Whom It May Concern:

We represent Atlantic General Hospital (“AGH”) located at 9733 Healthway Drive, Berlin, Maryland 21811, and are writing to notify your office of an incident that may affect the security of certain personal information relating to fifteen (15) New Hampshire residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, AGH 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 January 29, 2023, AGH discovered encrypted files on certain computer systems. AGH immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that there was unauthorized access to certain of AGH’s servers beginning on January 20, 2023. Through the investigation, AGH learned that certain files within its network were subject to unauthorized access during the period of unauthorized access. AGH then undertook a comprehensive review of these files to determine what data was contained within the files and to whom that data relates. On March 6, 2023, AGH determined that the impacted files contained certain sensitive information.

The information that could have been subject to unauthorized access for the New Hampshire residents includes
of the following:

Notice to New Hampshire Residents

On March 24, 2023, AGH provided written notice of this incident to fifteen (15) New Hampshire 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, AGH moved quickly to investigate and respond to the incident, assess the security of AGH systems, and identify potentially affected individuals. Further, AGH notified federal law enforcement regarding the event. AGH is also working to implement additional safeguards and training to its employees. AGH is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose Social Security number was potentially affected by this incident, at no cost to these individuals.

Additionally, AGH is providing impacted individuals with guidance on how to better protect against identity theft and fraud. AGH 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.

AGH is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. AGH is also notifying the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at

Very truly yours,

Paul T. McGurkin, Jr. of
MULLEN COUGHLIN LLC

PTM:bld
Enclosure

EXHIBIT A



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

To Enroll, Please Call:
1-888-338-9887
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

March 24, 2023

Notice of Data Event

Dear <<Full Name>>:

Atlantic General Hospital (“AGH”) writes to notify you of an incident that may affect the privacy of some of your information. We take this incident seriously. This letter provides details of the incident, our response, and steps you may take to better protect against possible misuse of your information, should you feel it appropriate to do so.

What Happened? On January 29, 2023, AGH 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 activity. Our investigation determined that there was unauthorized access to certain of our servers beginning on January 20, 2023. Through our investigation, we learned that certain files within our network were subject to unauthorized access during the period of unauthorized access. AGH then undertook a comprehensive review of these files to determine what data was contained within the files and to whom that data relates. On March 6, 2023, AGH determined that the impacted files contained certain information related to you. AGH has seen no evidence of misuse of any information related to this incident.

What Information Was Involved? AGH determined that the following information related to you was present on the impacted AGH servers: your name and <<data elements>>.

What We Are Doing. AGH takes the confidentiality, privacy, and security of information in our care seriously. 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.

AGH is providing you with access to <<12/24 months>> of credit monitoring and identity protection services through IDX at no cost to you. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Help Protect Personal Information*. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. AGH encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring free credit reports for suspicious activity and to detect errors. You can review the enclosed *Steps You Can Take to Help Protect Personal Information* for additional details on how to take steps to protect your information and enroll in complimentary credit monitoring, should you feel it is necessary to do so.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call 1-888-338-9887, Monday through Friday,

from 9:00 a.m. to 9:00 p.m. Eastern Time. Additionally, you can write to us at Atlantic General Hospital, Attention: Incident Response, 9733 Healthway Drive, Berlin, MD 21811.

AGH takes the privacy and security of the information in our care seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Donald R. Owrey
President & CEO
Atlantic General Hospital

Steps You Can Take to Help Protect Personal Information



1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll in services is June 24, 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 1-888-338-9887 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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
1-888-298-0045	1-888-397-3742	1-800-916-8800
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.

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 6 Rhode Island residents impacted by this incident.