MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

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

November 17, 2023

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Warren General Hospital ("WGH") located at 2 Crescent Park, Warren, PA 16365, and write to notify your office of an event that may have affected the security of certain personal information relating to approximately sixty-nine (69) New Hampshire residents. This notice may be supplemented if significant new facts are learned subsequent to its submission. By providing this notice, WGH 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 September 24, 2023, WGH identified suspicious activity on its network, including the malicious encryption of certain files. WGH immediately launched a comprehensive investigation, with the assistance of third-party cybersecurity and digital forensics specialists, to secure its systems and determine the nature and scope of the activity. WGH also prioritized the restoration of systems to minimize any impact to patient care and promptly reported the event to federal law enforcement. The investigation determined that an unknown actor accessed certain computer systems in WGH's network between September 15, 2023, and September 23, 2023, and acquired certain information from its network. In response, WGH undertook a comprehensive review of its internal records to determine what information was present on the affected systems and identify to whom it related and their contact information. WGH completed this review on or around October 31, 2023, and worked diligently to finalize and issue notifications to potentially affected individuals as expeditiously as possible.

The types of information involved for New Hampshire residents includes:

.

Notice to New Hampshire Residents

On November 17, 2023, WGH began providing written notice of this event to potentially affected individuals, including approximately sixty-nine (69) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***. WGH also issued notice on its website in substantially the same form as the notice attached hereto as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon identifying the event, WGH moved quickly to investigate and respond, assess the security of WGH systems, and identify potentially affected individuals. Further, WGH promptly reported the event to federal law enforcement. WGH also implemented additional administrative and technical safeguards. WGH is providing access to credit monitoring services for , through CyEx to individuals whose personal information was potentially affected by this event, at no cost to these individuals. WGH also established a toll-free assistance telephone line to address questions from notified individuals related to the event.

Additionally, WGH is providing potentially affected 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. WGH 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.

On November 9, 2023, WGH provided initial notice of this event to the U.S. Department of Health and Human Services. On November 17, 2023, WGH provided supplemental notice to the U.S. Department of Health and Human Services, as well as written notice to appropriate state privacy regulators, and to the three major consumer reporting agencies, Equifax, Experian, and TransUnion.

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,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/jc
Enclosure

EXHIBIT A

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Date>>

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

<<Variable Text – CA Header>>

Dear <<Name 1>>,

Warren General Hospital ("WGH") writes to inform you of a recent event that may affect the confidentiality of certain information related to you as a current or former WGH patient and/or current or former WGH employee. This letter provides information about the event, our response, and resources we are making available to you to help protect your information, should you determine it is appropriate to do so.

What Happened? On September 24, 2023, WGH identified suspicious activity on our network. We immediately took steps to secure our systems and launched an investigation into the nature and scope of the activity with the assistance of industry-leading cybersecurity specialists. We also promptly reported the event to federal law enforcement. The investigation determined that an unknown actor accessed certain computer systems in our network between September 15, 2023, and September 23, 2023, and downloaded certain information from our network. In response, we undertook a comprehensive review of our internal records to determine what information was present on the affected systems and identified contact information to provide notification to potentially impacted individuals. We recently completed this review.

What Information Was Involved? The type of information that may have been present on the impacted systems includes name, address, date of birth, Social Security number, financial account information, payment card information, health insurance claims information, and medical information including diagnosis, medications, lab results, and other treatment information.

What We Are Doing. We take this event and the security of personal information in our care very seriously. Upon learning of this event, we moved quickly to investigate and respond, assess the security of our network, and notify potentially affected individuals. As part of our ongoing commitment to information security, we reviewed existing policies and procedures, enhanced administrative and technical controls, and provided additional security training to reduce the likelihood of a similar future event. We also reported the event to appropriate governmental agencies, including federal law enforcement and U.S. Department of Health and Human Services. As an added precaution, we are offering complimentary credit monitoring and identity restoration services for <<12/24>> months through CyEx.

What You Can Do. We encourage you to remain vigilant against identity theft and fraud by reviewing your account statements, monitoring your free credit reports for suspicious activity, and to detect and report errors. We also encourage you to review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information.* There you will also find instructions on how to enroll in the credit monitoring and identity restoration services we are making available to you, free of cost.

For More Information. If you have additional questions, please call our toll-free assistance line at (888) 988-0582 between the hours of 9:00 a.m. and 9:00 p.m., Eastern time, Monday through Friday, excluding major U.S. holidays. WGH's mailing address is 2 Crescent Park West, Warren, PA 16365.

Sincerely,

Richard Allen
Chief Executive Officer
Warren General Hospital

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

Identity Defense

Enter your Activation Code: <<ActivationCode>>
Enrollment Deadline: <<Deadline Date>>
Service Term: <<12/24>> months*

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit https://app.identitydefense.com/enrollment/activate/warr

1. **Enter your unique Activation Code** <<ActivationCode>>
   Enter your Activation Code and click 'Redeem Code'.
2. **Create Your Account**
   Enter your email address, create your password, and click 'Create Account'.
3. **Register**
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. **Complete Activation**
   Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Deadline Date>>. After <<Deadline Date>>, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by <<Deadline Date>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.800.297.6399.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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

Consumers may further educate themselves 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 their 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers 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, consumers will likely need to provide some proof they 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, D.C. 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; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There are approximately <<RI #>> Rhode Island resident that may be impacted by this event.

EXHIBIT B

November 9, 2023 – Warren General Hospital ("WGH") is issuing notice of a recent data security event that potentially affected the confidentiality of information related to certain current and former WGH patients and/or current and former WGH employees. We are providing information about the event, our response, and steps potentially affected individuals may take to better protect against the possibility of identity theft and fraud, should they feel it is appropriate to do so.

What Happened? On September 24, 2023, WGH identified suspicious activity on our network. We immediately took steps to secure our systems and launched an investigation into the nature and scope of the activity with the assistance of industry-leading cybersecurity specialists. We also promptly reported the event to federal law enforcement. The investigation determined that an unknown actor accessed certain computer systems in our network between September 15, 2023, and September 23, 2023, and downloaded certain information from our network. In response, we undertook a comprehensive review of our internal records to determine what information was present on the affected systems and identified contact information to provide notification to potentially impacted individuals. We recently completed our review.

What Information Was Affected. The types of information that may have been present on the impacted systems includes

.

What We Are Doing. We take this event and the security of personal information in our care very seriously. Upon learning of this event, we moved quickly to investigate and respond, assess the security of our network, and notify potentially affected individuals. As part of our ongoing commitment to information security, we reviewed existing policies and procedures, enhanced administrative and technical controls, and provided additional security training to reduce the likelihood of a similar future event. We also reported the event to appropriate governmental agencies, including federal law enforcement and U.S. Department of Health and Human Services.

What Affected Individuals Can Do. As a precautionary measure, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing account statements, credit reports, and explanations of benefits for unusual activity and to detect errors. Any suspicious activity should be promptly reported to your insurance company, health care provider, or financial institution. Additional information can be found below in the *Steps You Can Take to Help Protect Personal Information.*

For More Information. If you have additional questions, you may call our toll-free assistance line at (888) 988-0582 between the hours of 9:00 a.m. and 9:00 p.m., Eastern time, Monday through Friday, excluding major U.S. holidays. You may also write to WGH at 2 Crescent Park, Warren, PA 16365.

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL 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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers 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 one-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 consumers 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 a consumers name without consent. You should be aware; however, 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, consumers cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, consumers 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 consumers 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

Consumers may further educate themselves 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 their 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. To file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the consumer's 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 https://www.marylandattorneygeneral.gov/

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. Fees may be required to be paid to the consumer reporting agencies. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event.