BakerHostetler

Baker&Hostetler LLP

1735 Market Street
Suite 3300
Philadelphia, PA 19103-7501

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Sara Goldstein
direct dial: 215.564.1572
sgoldstein@bakerlaw.com

December 21, 2021

VIA E-MAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General John M. Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Formella:

We write on behalf of our client, Monongalia Health System, Inc., and its affiliated hospitals, Monongalia County General Hospital Company and Stonewall Jackson Memorial Hospital Company (collectively, "Mon Health"), to notify you of a data security incident.

On October 29, 2021, Mon Health completed its investigation of an email phishing incident which may have resulted in unauthorized access to emails and attachments in several Mon Health email accounts that contain information pertaining to patients of Mon Health's affiliated hospitals, Monongalia County General Hospital Company and Stonewall Jackson Memorial Hospital. Mon Health first became aware of the incident after a vendor reported not receiving a payment from Mon Health on July 28, 2021. The vendor's report prompted Mon Health to look into the missing payment further. Through this review, Mon Health determined that unauthorized individuals had gained access to a Mon Health email account and sent emails from the account in an attempt to obtain funds from Mon Health through fraudulent wire transfers.

Upon learning of this, Mon Health then promptly secured the Mon Health email account, notified law enforcement, and launched an investigation with the assistance of a third-party forensic firm. The investigation confirmed that this incident was limited to Mon Health's email system and did **not** involve Mon Health's electronic health records systems. Importantly, this incident did **not** disrupt the services or operations of Mon Health or its affiliated hospitals.

Mon Health's investigation determined that unauthorized individuals accessed certain Mon Health email accounts between the dates of May 10, 2021 and August 15, 2021. In response, Mon Health secured the email accounts.

Based on its investigation, the likely purpose of the unauthorized access to the email accounts was to obtain funds from Mon Health through fraudulent wire transfers and to perpetrate an email phishing scheme, not to access personal information. That said, Mon Health cannot rule out the possibility that emails and attachments in the involved Mon Health email accounts may have been viewed or accessed as a result of this incident. Thus, out of an abundance of caution, Mon Health conducted a comprehensive search of the emails and attachments in the involved email accounts.

Through this search, Mon Health determined that emails and attachments that may have been accessed as a result of the incident contain information pertaining to current and former Mon Health patients. For Mon Health patients, this information included names and medical record numbers, and may have also included addresses, dates of birth, patient account numbers, Medicare Health Insurance Claim Numbers (which could contain Social Security numbers), health insurance plan member ID numbers, dates of service, provider names, claims information, medical and clinical treatment information and/or status as a current or former Mon Health patient.

Beginning on December 21, 2021, Mon Health will mail notification letters via United States Postal Service First-Class mail to individuals whose information may have been involved in this incident, including 12 New Hampshire residents[1][2], in accordance with N.H. Rev. Stat. Ann. § 359-C:20 and 45 C.F.R. § 164.404. A copy of the notification letter is enclosed.[3] Mon Health is offering individuals whose Social Security numbers or Medicare Health Insurance Claim Numbers (which could contain Social Security numbers) may have been involved complimentary one-year memberships to credit and identity monitoring services through Experian. Mon Health has also established a dedicated, toll-free incident response line to answer questions about the incident.

To help prevent something like this from happening again, Mon Health is continuing to review and enhance its existing security protocols and practices, including the implementation of multi-factor authentication for remote access to its email system.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Sara Goldstein

Sara M. Goldstein
Partner

Enclosure

[1] In addition, Mon Health is also providing notification of this incident to an additional 38 New Hampshire residents whose names, addresses, dates of birth, Medicare Health Insurance Claim Numbers (which could contain Social Security numbers), patient account numbers, health insurance plan member ID numbers, medical record numbers, dates of service, provider names, claims information and/or medical and clinical treatment information may have been accessed as a result of this incident, in accordance with 45 C.F.R. § 164.404.
[2] The addresses are being run through the United States Postal Services' National Change of Addresses Database. Therefore, the total number of notified residents in your state may change.
[3] This report does not waive Mon Health's objection that New Hampshire lacks personal jurisdiction over it related to any claims that may arise from this incident.

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

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Monongalia Health System, Inc., including its affiliated hospitals Monongalia County General Hospital Company and Stonewall Jackson Memorial Hospital Company (collectively, "Mon Health") is committed to enhancing the health of the communities we serve, one person at a time, and protecting the privacy and security of the information we maintain. We are writing to notify you of a data security incident that may have involved some of your information. This notice explains the incident, measures we have taken, and steps you can take in response.

What Happened: On October 29, 2021, Mon Health determined that an email phishing incident may have resulted in unauthorized access to emails and attachments in several Mon Health email accounts. Mon Health first became aware of the incident after a vendor reported not receiving a payment from Mon Health on July 28, 2021. In response, Mon Health promptly launched an investigation, through which it determined that unauthorized individuals had gained access to a Mon Health contractor's email account and sent emails from the account in an attempt to obtain funds from Mon Health through fraudulent wire transfers.

Upon learning of this, Mon Health secured the contractor's email account and reset the password, notified law enforcement, and a third-party forensic firm was engaged to assist with the investigation. The investigation confirmed that this incident was limited to Mon Health's email system, and did **not** involve Mon Health's electronic health records systems. Importantly, this incident did **not** disrupt the services or operations of Mon Health or its affiliated hospitals.

Through our investigation, we identified unauthorized access to several Mon Health email accounts between the dates of May 10, 2021 and August 15, 2021. In response, Mon Health secured the email accounts and reset their passwords.

Based on our investigation, we believe the purpose of the unauthorized access to the Mon Health email accounts was to obtain funds from Mon Health through fraudulent wire transfers and to perpetrate an email phishing scheme, not to access personal information. That said, we cannot rule out the possibility that emails and attachments in the Mon Health email accounts containing information pertaining to Mon Health patients, providers, employees, and contractors may have been accessed as a result of this incident. Thus, out of an abundance of caution, we conducted a comprehensive search of the contents of those email accounts to identify the information they contained.

What Information Was Involved: Through our investigation, we determined that this incident may have resulted in unauthorized access to emails and/or attachments that contain your name and medical record number, and may have also contained your address, date of birth, patient account number, health insurance plan member ID number, dates of service, provider names, claims information, medical and clinical treatment information, and/or status as a current or former Mon Health patient. In addition, your Medicare Health Insurance Claim Number (HICN), which may contain your Social Security number, may have been involved.

What We Are Doing: To help prevent a similar incident from occurring in the future, we are continuing to enhance our existing security protocols and practices, including the implementation of multi-factor authentication for remote access to our email system.

What You Can Do: Although, to date, we are unaware of any misuse of personal information as a result of this incident, we recommend that you review the statements you receive from your healthcare providers and health insurance plan. If you see any services that were not received, you should contact the relevant provider or health plan immediately. Additionally, we encourage you to remain vigilant to the possibility of fraud by reviewing your financial account statements for any suspicious activity. If you identify any suspicious activity, you should notify your financial institution immediately. As a precaution, we are also offering you a complimentary one-year membership to Experian's® IdentityWorks℠. This product helps detect potential misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks is completely free and it is our understanding that enrolling in this program will not hurt your credit score. **For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take to protect your information, please see the pages that follow this letter.**

For More Information: We regret any inconvenience or concern this incident may cause. If you have any questions, please call our dedicated assistance line at (855) 545-2461, Monday through Friday, between 9:00 a.m. and 6:30 p.m., Eastern Time (except for on major U.S. holidays).

Sincerely,

David S. Goldberg

David S. Goldberg
President and CEO
Monongalia Health System, Inc.

To help protect your identity, we are offering a **complimentary one-year** membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **<<b2b_text_6(activation deadline)>>** (Your code will not work after this date.)

2.VISIT the **Experian IdentityWorks website** to enroll: **URL**

3. PROVIDE the **Activation Code**: **<<activation code s_n>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **PHONE NUMBER**. Be prepared to provide engagement number **<<b2b_text_1(engagement number)>>** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12 MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at URL
or call PHONE NUMBER to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at **PHONE NUMBER**.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Maryland Residents: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York Residents: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina Residents: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island Residents: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia Residents: You have the right to ask that nationwide consumer reporting agencies place «fraud alerts» in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.