Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

31149

[redacted]

December 8, 2023

Notice of Perry Johnson & Associates Data Breach

Dear [redacted]:

We are writing to inform you that Perry Johnson & Associates ("PJA") experienced a data security issue. PJA is a former third-party vendor that provided Mercy and numerous other hospitals across the country with transcription services for the purposes of transcribing provider-patient interactions. We worked with PJA for these services from May 2, 2011 to May 31, 2014. We were recently notified by PJA that a data security incident affecting their computer systems may have resulted in unauthorized access to your information.

We take the security of your information seriously and want to provide you with information and resources you can use to protect your information.

What Happened:

On May 2, 2023, PJA discovered a potential security incident involving an unauthorized individual who may have gained access to some of its systems. The unauthorized individual claimed to have obtained access to the systems and demanded a ransom payment. According to PJA, they immediately launched an investigation, retained a third-party cybersecurity expert to aid in its investigation, and worked with that expert to ensure that the threat was contained and that PJA's systems were secured.

According to PJA, they then began working to determine whether any unauthorized access occurred, and to determine the scope of any such access. On May 22, 2023, they initially identified that the unauthorized individual had gained access to a database containing customer information. Since that date, they have continued the investigation and worked to identify the scope of affected customer data and notified law enforcement authorities of the event. On August 16, 2023, PJA determined that the unauthorized individual had obtained the complete backup files for a database which contained customer data for several organizations, including Mercy Medical Center. Specifically, they determined that the individual obtained those backup files on April 7, 2023 and accessed them again on April 19, 2023. On October 5, 2023, PJA determined that Mercy Medical Center data was affected, and PJA notified us on October 10, 2023. We have performed our own investigation and completed the tasks necessary to provide this notification to you.

What Information Was Involved:

PJA's investigation concluded that, by obtaining the above-referenced backup files, the unauthorized individual obtained Mercy Medical Center data which was likely originally associated with a transcription request, although no transcription data was found at the time of the investigation. The data would have included patient data such as Name, Date of Birth, Address, Social Security Number, Medical Record Number, Patient Account Number, and Dates of Admission, Discharge, and Exam.

What We Are Doing:

We want you to know Mercy Medical Center takes this situation seriously. While our relationship with PJA ended in 2014, we have opened an inquiry to determine why the information remained in their systems. We hold our vendors to high data security and privacy standards and will continue to do so going forward.

Also, we recommend you remain vigilant by reviewing account statements and monitoring free credit reports and promptly report any suspicious activity or suspected identity theft to law enforcement authorities. Please know that Mercy Medical Center will never solicit sensitive information from you via email or telephone.

To help protect your information, we are offering you access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. Instructions on how to enroll in these services are included in this letter, along with additional information regarding the resources available to you, and the steps you can take to further protect your personal information.

We sincerely apologize for any concern or inconvenience this issue may cause you and assure you that protecting your information is of utmost importance to us. If you have any questions or need assistance, please call us at (866) 409-9434 between the hours of 6:00 am and 6:00 pm (CDT) Monday through Friday.

Sincerely,

Julie Thompson
Privacy Officer
Mercy Medical Center

MERCY-ADT-2YR

Additional Information

Credit Monitoring: To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/mercymedical** and follow the instructions provided. When prompted, please provide the following unique code to receive services: [redacted].

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It isessential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960
https://www.equifax.com/personal/credit-report-services/credit-freeze/

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center html

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-909-8872
www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- *Equifax* (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- *TransUnion* (https://www.transunion.com/fraud-alerts); or
- *Experian* (https://www.experian.com/fraud/center.html).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at listed above.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding preventing identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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 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. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 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 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 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 violators. 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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and https://ag.ny.gov/.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 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.