Perry Johnson & Associates
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

February 5, 2024

Re: NOTICE OF DATA INCIDENT

Dear :

Perry Johnson & Associates ("PJ&A") provides this letter to notify you about a data security incident ("incident"), which may have affected the privacy and security of your personal health information. The letter describes the incident and our response to the incident. It also describes resources which will be made available to you, which may help protect your personal health information from potential misuse.

What Is PJ&A? PJ&A is a former vendor to The South Bend Clinic, LLC (collectively, ("SBC")). Specifically, PJ&A provided certain transcription, dictation, and related services to SBC. In order to provide these services, PJ&A received personal health information from SBC about its patients.

What Happened? On May 2, 2023, PJ&A became aware of a potential data security incident impacting PJ&A's systems. Thereafter, PJ&A immediately launched an internal investigation and retained a cybersecurity vendor to assist with the investigation, contain the threat and further secure its systems. On May 22, 2023, PJ&A preliminarily determined that an unauthorized third party had accessed PJ&A data and that SBC data was likely impacted by this event, although further investigation would be required to determine the scope of the impacted data. Although the investigation was ongoing, on September 11, 2023, PJ&A provided initial notification regarding the data security incident to SBC, based on the information known at that time.

By December 22, 2023, PJ&A provided the final results of its investigation as to the specific impacted personal health information for affected SBC customers. The investigation ultimately determined that the unauthorized access to PJ&A systems occurred between March 27, 2023, and May 2, 2023, and that unauthorized access to personal health information, including SBC information, occurred between April 7, 2023, and April 19, 2023, with certain subsets of data accessed for shorter periods during this timeframe.

What Information Was Involved? PJ&A has confirmed that a database containing your personal health information was impacted by this incident. Specifically, the following information of yours may have been impacted: your name
Social Security numbers were not impacted as a result of this incident.

What Actions Did We Take? PJ&A is committed to maintaining the privacy and security of your information and we take this incident very seriously. PJ&A has taken, and will continue to take, appropriate steps to address this incident, including further enhancing our security systems to prevent incidents of this nature from occurring in the future.

As soon as PJ&A learned of the potential unauthorized access to our systems, it immediately initiated an investigation and retained a cybersecurity vendor to assist with containing the threat and with further securing our systems.

PJ&A also notified law enforcement about the incident and will continue to cooperate with law enforcement's investigation. PJ&A further implemented additional technical restrictions in our systems, and required a password reset for all employees. Additionally, with the assistance of our cybersecurity vendor, PJ&A deployed an endpoint detection and response system to monitor any unauthorized access of our systems. PJ&A has also taken additional steps to ensure that no patient data was made public, and, to date, it has not identified any evidence that the unauthorized actor has further disclosed and/or made any observable use of the data.

What Can You Do? We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, which includes further information on what you can do to protect your information against misuse, should you feel it necessary to do so.

For More Information. The privacy and security of your personal health information is of the utmost importance to us. If you have additional questions, please call our dedicated assistance line at 833-200-3558 and select option 8. The dedicated assistance line is available Monday through Friday from 8:00 am to 11:59 pm Eastern Time (excluding major US holidays). We sincerely regret this occurrence and apologize for any inconvenience or concern that it may cause you.

Sincerely,

PJ&A

Enclosure

STEPS YOU CAN TAKE TO HELP PROTECT YOUR 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 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 they 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, D.C. 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. Please note that in order 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 relevant 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 https://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. There are approximately 12 Rhode Island residents that may be impacted by this event.