WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

April 8, 2022

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Certified Mail; Return Receipt Requested:

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

Re: Cybersecurity Incident Involving New Jersey Brain & Spine

Dear Attorney General Formella:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents New Jersey Brain & Spine ("NJBS"), a neurosurgical clinic located at 680 Kinderkamack Rd Suite 300, Oradell, NJ 07649, with respect to a recent cybersecurity incident that was first discovered by NJBS on November 16, 2021 (hereinafter, the "Incident"). NJBS takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of New Hampshire residents being notified, and the steps that NJBS has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On November 16, 2021, NJBS discovered the Incident when an employee noticed read-me text file indicating that an unauthorized individual allegedly stole NJBS data. Upon discovery of the incident, NJBS promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. The forensic investigation found there was evidence that some of NJBS's data may have been accessed by an unauthorized individual. NJBS immediately began a thorough review of the potentially accessed files to identify the individuals whose sensitive information may have been compromised.

2. Nature of Personal Information

Although NJBS is unaware of any fraudulent misuse of information, it is possible that individuals' full name, address, social security number, financial account information, driver's license or other ID number, credit or debit card number, username ID and password information, and/or health information may have been exposed as a result of this unauthorized activity.

As of this writing, NJBS has not received any reports of related identity theft since the date of the Incident (November 16, 2021 to present).

3. Number of New Hampshire residents affected.

A total of eleven (11) New Hampshire residents have been potentially affected by this incident. Notification letters to individuals were mailed on April 8, 2022, by first class mail. A sample copy of the notification letter is included with this letter under **Exhibit A.**

4. HIPAA Substitute Notice

Since NJBS did not have addresses for all affected individuals, NJBS also posted notice of this Incident on its website on March 10, 2022 pursuant to HIPAA's Substitute Notice requirement, in addition to Media Notice sent to the New York Post, the New Jersey Star-Ledger, and the Tampa Bay Times.

5. Steps taken in response to the Incident.

NJBS is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, NJBS moved quickly to investigate and respond to the Incident, assessed the security of its systems, and will be notifying the potentially affected individuals. Specifically, NJBS engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, NJBS has migrated to a third-party hosted cloud-based platform to securely store patient data, implemented two-factor authentication, installed a new server, and implemented ongoing monitoring response which tracks user activity, services and ports and coordinates logging.

Although NJBS is not aware of any actual or attempted misuse of the affected personal information, NJBS will be offering twelve (12) months of complimentary credit monitoring and identity theft restoration services to individuals to help protect their identity. Additionally, NJBS provided guidance on how to better protect against identity theft and fraud, including providing 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 the contact details for the Federal Trade Commission.

6. Contact information

NJBS remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

EXHIBIT A

NEW JERSEY
BRAIN AND SPINE
P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-774-1217
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<Enrollment>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

April 7, 2022

Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

New Jersey Brain & Spine ("NJBS") is writing to inform you of a recent cybersecurity incident ("Incident") that may have involved your protected health information. NJBS takes the privacy of patient information very seriously and sincerely apologizes for any inconvenience this Incident may cause. This letter contains details about the Incident, steps we have taken in response to mitigate any risk, and services we are making available to protect your information.

What Happened?

On or about November 16, 2021, NJBS first discovered that it was the victim of a cyber attack which may have resulted in unauthorized access to patient information stored on our systems. After learning about this Incident, NJBS promptly engaged a third party cybersecurity firm to conduct a forensics investigation to analyze the nature and scope of the Incident, and to determine whether any patient information may have been exposed as a result. The forensic investigation completed on January 25, 2022 which concluded that an unauthorized individual accessed patient information on NJBS' systems. On March 10, 2022, NJBS finalized the notification population.

What Information Was Involved?

The investigation confirmed that patient information stored on one our systems may have been subject to unauthorized access. The data contained in this system may include protected health information such as: names, addresses, email addresses, dates of birth, telephone numbers, social security numbers, financial account information, credit or debit card numbers, driver's license numbers or other ID numbers, user ID and password information, and medical information. Please note that not every element was present for every individual.

While NJBS has no reason to believe that any patient's information has been misused, we are nonetheless notifying our patients out of an abundance of caution.

What We Are Doing

NJBS takes the privacy and security of our patient information very seriously, and has taken steps to prevent a similar event from occurring in the future. In response to the Incident, NJBS has migrated to a third-party hosted cloud-based platform to securely store patient data, implemented two-factor authentication, installed a new server, and implemented ongoing monitoring response which tracks user activity, services and ports and coordinates logging.

In order to address any patient concerns and mitigate any exposure or risk of harm following this Incident, NJBS has arranged for IDX to provide complimentary credit monitoring services and identity theft protection services to our patients free of charge for a period of twelve (12) months.

What You Can Do

Although NJBS is not aware of any instances of misuse of any patient information, we recommend that our patients take advantage of the complimentary services that are being offered. To enroll, please call 1-833-774-1217 or visit https://app.idx.us/account-creation/protect. Please note the deadline to enroll in these services is July 7, 2022. We also encourage our patients to remain vigilant and review the enclosed addendum titled "*Additional Important Information*" outlining additional steps you can take to protect your information.

For More Information

NJBS recognizes that you may have questions not addressed in this letter. If you have additional questions, please call 1-833-774-1217 (toll free) during the hours of 9 a.m. and 9 p.m. Eastern Time, Monday through Friday (excluding U.S. national holidays).

NJBS sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Jonathan Tamir

Jonathan Tamir
CEO
NJ Brain and Spine

Additional Important Information

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.

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

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Identity Protection PIN: You can get a six-digit Identity Protection PIN to prevent someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. An IP PIN is used by the IRS to verify your identity when filing your electronic or paper tax return. To receive an IP Pin, you must register to validate your identity at IRS.gov. Use the Get an IP PIN tool available between mid-January through mid-November to receive your IP PIN.

https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin

Security Freeze: You 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 is essential 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:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order 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 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. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a 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 residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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 at 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 residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of *Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island*:
You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov