



Midwest Spine And Brain Institute **Notice of Data Security Incident**

Midwest Spine And Brain Institute (“MSBI”) is committed to our patients. Protecting the privacy and security of your personal information is of the utmost importance to MSBI. As such, we are writing with important information regarding a network security incident involving our third-party provider, 3C Care Systems, LLC (“3C”).

MSBI recently learned that its third-party MSP provider, 3C, was affected by an external cyber-attack. 3C is a healthcare IT company specializing in workflow automation and augmentation solutions. Upon learning of the issues with 3C, MSBI immediately opened an investigation with the assistance of external professional experienced in handling these types of incidents to assist us with an investigation and to assess the full scope of information impacted. 3C also conducted an independent, external forensic investigation with the assistance of cybersecurity professionals. At this time, we can confirm there was no compromise to MSBI’s larger network due to this incident.

MSBI’s review determined that the potentially impacted information included first and last names with one or more of the following identifiers: date of birth, medical treatment, procedure, and/or diagnosis information, medical record number, medical provider information, medical prescription information, dates of service, and health insurance claim and/or policy information. Our investigation is still ongoing. As such, we have not confirmed whose personal information may have been impacted. However, in general, the potentially impacted information could include protected health information (“PHI”) and personally identifiable information (PII). The types of impacted information varied by individual and not all of these data elements were impacted for each individual.

When the investigation concludes, MSBI will provide written notice of this incident via U.S. mail to affected individuals for whom it has a last known address. The notice contains information about the incident, as well as information and resources to help individuals protect their information. Out of an abundance of caution, we will offer complimentary identity monitoring and protection services for individuals whose Social Security number was involved in this incident.

Thank you for your continued trust in MSBI. MSBI takes this matter seriously. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of the information we maintain, and we are taking steps to mitigate the risk to persons impacted by this incident. If you have any questions regarding this incident, please contact HIPAA@midwestspine.net.

Sincerely,

MSBI

Steps Individuals Can Take to Protect Personal Information

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion
Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

2. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(800) 349-9960
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Protecting Your Medical Information.

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.