December 5, 2022 – Mississippi Sports Medicine and Orthopaedic Center (“MSMOC”), is updating and supplementing our previous May 2022 notice of a data security event that may impact information related to certain patients. We are providing information about the event, measures we have taken in response, and steps potentially impacted individuals can take to better protect against the possibility of identity theft and fraud, should they feel it is necessary to do so.

**What Happened?** On March 9, 2022, MSMOC became aware of suspicious activity within its computer network, including the unauthorized encryption of certain data. Steps were promptly taken to secure MSMOC’s network, and an investigation began with the assistance of outside cybersecurity specialists to determine the nature and scope of this activity and restore full functionality to MSMOC’s operations as quickly as possible. This investigation found that certain files from within MSMOC’s network were potentially viewed and/or taken by an unauthorized actor between March 3, 2022, and March 9, 2022. Additionally, on March 11, 2022, we determined that certain patient records were inaccessible after our medical records system was restored from backups. In response, our physicians and staff used available information to restore access to and/or recreate as many patient records as possible, including notes within patient charts.

We then conducted a thorough and lengthy review of the affected files to determine whether any potentially sensitive information was present within them and to identify those patients who were impacted by this event. We recently concluded this review and are mailing letters to potentially affected individuals.

**Which Patients / What Information was Affected?** The information potentially impacted by this event varies per individual and is specified in the letters sent to the affected individuals. It is important to know that not all patients were impacted by this event, and not all impacted patients had the same types of information involved. If you were impacted and received a letter, please consult the “What Information Was Involved?” paragraph of your letter. If you did not receive a letter, but think you may be affected, please call our assistance line at the number in the “For More Information” section below.

The patient records which are inaccessible and unable to be recovered concern records created between February 28, 2022, and March 8, 2022. The types of impacted records may vary by patient and include the following: doctor’s and/or surgical notes; patient appointment records; X-ray, MRI, and/or surgical images; certain billing information; and prior authorization records.

The types of information related to patients and potentially impacted by the unauthorized network activity include: name, Social Security number, address, telephone number, email address, date of birth, medical record number, health plan beneficiary number, signature, and medical and/or clinical information including diagnosis and treatment history, disability information, physician name, and health insurance information.

**What We are Doing.** MSMOC takes this event and the security of your information seriously. Upon learning of this event, we immediately took steps to restore our operations and further secure our systems. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional administrative and technical safeguards to further secure the information in our systems. Notice was also provided to federal law enforcement and the U.S. Department of Health and Human Services.

**What Affected Individuals Can Do.** Potentially affected current and former patients of MSMOC are encouraged to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity and report any suspicious activity promptly to your insurance company, health care provider, or financial institution. Additional detail can be found below in the *Steps You Can Take to Help Protect Your Information* and in the notification letters sent to affected individuals.

**For More Information.** If you have additional questions, please call our assistance line at (800) 624-9168, 7:00am CT – 5:00pm CT, Monday through Friday. You may also write to MSMOC at 1325 East Fortification St., Jackson, MS 39202, Attn: Compliance Officer.

**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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 one-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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, 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 | 1-833-395-6938 |
| 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**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General.The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. 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 in order 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 and your state Attorney General. This notice has not been delayed by law enforcement.

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and [www.oag.state.md.us](http://www.oag.state.md.us).

*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 [www.ncdoj.gov](http://www.ncdoj.gov/).