Orthopaedic Outpatient Surgery Center, L.C. Health Provides Notice of Data Security Incident

The privacy and security of protected health information is of the utmost importance to Orthopaedic Outpatient Surgery Center, L.C. ("OOSC"). This notice contains information regarding a data security incident that involved certain protected health information collected and maintained by Des Moines Orthopaedic Surgeons, P.C. ("DMOS"), whichis part of a joint venture with OOSC. DMOS, on behalf of OOSC, is providing individuals with information about the incident and the services being made available to those who are involved. DMOS continues to take significant measures to protect personal information.

DMOS experienced a security incident that impacted its network on or about February 17, 2023, when an unauthorized actor was able to access and/or remove certain DMOS files from its network due to a DMOS vendor failure. Upon learning of this issue, DMOS immediately contained the threat and commenced a prompt and thorough investigation. As part of the investigation, DMOS engaged external cybersecurity professionals who regularly investigate and analyze these types of situations to help determine the extent of any compromise of the information on the DMOS network. DMOS also notified law enforcement of the incident and changed cybersecurity vendors supporting their network security. DMOS devoted considerable time and effort to assessing the extent and scope of the incident and to determine what information may have been accessible to the unauthorized users. Based on the comprehensive investigation, DMOS concluded that certain OOSC documents and records maintained within its possession was compromised in connection with this incident. OOSC determined on January 8, 2024 that certain OOSC personal and health information was present in the impacted documents and records. The impacted data includes full names in combination with one or more of the following: Social Security numbers, date of birth, driver's license numbers and/or state identification numbers, passports, direct deposit bank information, medical information and health insurance information. Not all data elements were impacted for every individual.

To date, DMOS is not aware of any incidents of identity fraud or financial fraud as a result of the incident. Nevertheless, out of an abundance of caution, DMOS, on behalf of OOSC, is providing notice to the individuals whose information was potentially involved. DMOS mailed notification to all individuals it has contact information for on file, via U.S. mail on January 22, 2024. Notified individuals may take steps to protect themselves including placing a fraud alert/security freeze on their credit files, obtaining free credit reports, and remaining vigilant in reviewing financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis. In addition, individuals who may have had their Social Security number involved are encouraged to enroll in complimentary credit monitoring services provided in the notification letter.

Individuals who have questions or need additional information regarding this incident or to determine if they are notified may reach out to the toll-free response line that DMOS has set up to respond to questions at 1-888-983-0228. This response line is available Monday through Friday 9:00 a.m. – 9:00 p.m. Eastern Time (excluding major U.S. holidays).

– OTHER IMPORTANT INFORMATION –

1. <u>Placing a Fraud Alert on Your Credit File.</u>

You may 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 Fraud Alert on Your Credit File.

You may 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

3. 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
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

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.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. 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.

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 this notice letter states that 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.

6. Protecting Your Medical Information.

We have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from 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.