Orthopedic Associates of Duchess County Provides Notice of a Security Incident

Orthopedic Associates of Dutchess County ("OADC") is providing notice of a recent incident that may affect the security of certain information relating to current and former patients.

What Happened? On March 5, 2021, OADC became aware of suspicious activity relating to its systems and immediately launched an investigation to determine the nature and scope of the activity. OADC determined that an unauthorized actor gained access to certain OADC systems on or about March 1, 2021, encrypted certain systems, and claims to have removed and/or viewed certain files.

Although the investigation has been unable to confirm the full scope of files that were actually removed and/or viewed by an unauthorized actor or which specific files may have been impacted, we could not rule out the possibility that some individuals' information was or may have been viewed or taken. Therefore, in an abundance of caution, OADC reviewed the information that is housed on its systems. The initial review determined that certain information related to individuals was or may have been impacted.

What Information was Involved? The following types of information that OADC maintains in its systems and that were, or may have been, impacted by this incident include individual's name, address, telephone number, email address, emergency contact, guarantor, patient identification number, medical record number, diagnosis information, health insurance number and other health insurance information, payment details, date of birth, Social Security number, and treatment information. To date, OADC has not received any reports of fraudulent misuse of any information potentially impacted.

What is OADC Doing? OADC takes this incident and security of personal information in its care seriously. OADC moved quickly to investigate and respond to this incident, assess the security of relevant OADC systems, and notify potentially affected individuals. In response to this event, OADC is reviewing and enhancing existing OADC policies and procedures. OADC notified the Federal Bureau of Investigation ("FBI") and the Department of Health and Human Services of this incident. OADC is also notifying potentially impacted individuals so that they may take further steps to protect their information, should they feel it appropriate to do so.

What Can Impacted Individuals Do? OADC has established a dedicated assistance line for individuals seeking additional information regarding this incident. Individuals seeking additional information may call the toll-free assistance line at (855) 246-9403. This toll-free line is available Monday – Friday from 9:00 am ET to 11:00 pm ET and Saturday – Sunday from 11:00 am ET to 8:00 pm ET. Individuals may also write to OADC at 1910 South Road. Poughkeepsie, NY 12601 with questions.

Potentially affected individuals may also consider the information and resources outlined below. OADC encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud and to review account statements, credit reports, and explanation of benefits forms for suspicious activity and report any suspicious activity immediately to their insurance company, health care provider, or financial institution.

Steps You Can Take To Protect Your Personal Information

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. Individuals 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 an individual is the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should they wish to place a fraud alert, they may 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 an individual's name without their consent. However, individuals 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, an individual cannot be charged to place or lift a credit freeze on their credit report. To request a security freeze, individuals 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 they are a victim of identity theft.

Should individuals wish to place a fraud alert or credit freeze, they may 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
888-298-0045	1-888-397-3742	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

Individuals may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their 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, 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. Individuals can obtain further information on how to file such a complaint by way of the contact information listed above. Individuals 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, individuals 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 their state Attorney General. This notice has not been delayed by law enforcement.