TOA

TENNESSEE ORTHOPAEDIC ALLIANCE

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notification of Data Security Incident

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

We are writing to inform you of a data security incident experienced by Tennessee Orthopaedic Alliance ("TOA") that may have affected your personal or health information. TOA takes the privacy and security of patient information very seriously and deeply regrets any concern that this incident may cause. We are writing to notify you of this incident and to inform you about steps that can be taken to help protect your information.

What Happened? On October 18, 2019, TOA discovered unusual activity in an employee's email account. TOA immediately took steps to secure its email system and launched an investigation with the assistance of a leading digital forensics firm to determine whether additional email accounts may have been impacted and whether any personal information was accessed or acquired without authorization. Through this investigation, TOA learned that an email account belonging to a second employee may have been impacted as well. The two email accounts were subject to authorized access by an unknown party between August 16 and October 14, 2019. On January 3, 2020, our investigation determined that your information was contained in the impacted accounts and therefore may have been viewed or accessed without authorization, though the investigation could not conclude definitively whether your information was actually accessed or acquired. TOA then worked to identify up-to-date address information required to notify potentially impacted individuals.

Please note that this incident was limited to information transmitted via email and did not affect any other information systems. Moreover, we have no evidence to suggest your personal information has been misused. Nonetheless, out of an abundance of caution, TOA is notifying you of this incident and providing you with information about steps you can take to help protect your information.

What Information Was Involved? The information may have included your name, contact information (such as address, phone number and email address), date of birth, health insurance information, treatment or diagnostic information (including codes), and/or treatment cost information. Your Social Security number was not impacted in connection with this incident.

What We Are Doing. As soon as we discovered this incident, we took the measures referenced above. We also implemented enhanced security measures in order to better safeguard all personal information in our possession and to help prevent a similar incident from occurring in the future. In addition, we reported this matter to the Federal Bureau of Investigation and will provide whatever assistance is necessary to hold the perpetrators of this incident accountable. Additionally, out of an abundance of caution, we are providing you with information about steps you can take to help protect your information.

What You Can Do. We recommend that you review the guidance included with this letter about how to protect your personal information.

For More Information. If you have questions or need assistance, please contact Kroll at 1-844-936-0059, Monday through Friday from 8 a.m. to 5:30 p.m. Central Time. Our representatives are fully versed on this incident and can answer any questions you may have regarding how to help safeguard your personal information.

Thank you for your patience through this incident. We take your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Rob Simmons
Chief Executive Officer
Tennessee Orthopaedic Alliance

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.