



Keeping you active.

17108

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notification of Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a potential data security incident Florida Orthopaedic Institute ("FOI") recently discovered that may have involved your personal information. At FOI, we take the privacy and security of all patient information very seriously. This letter contains information about steps you can take to help protect your information and resources we are making available to help you.

What Happened? On or about April 9, 2020 we discovered that we were the victim of a ransomware attack that encrypted the data stored on our servers. We immediately began an internal investigation to secure our environment and restore impacted data. We also engaged a third-party forensic investigator to assist us with the investigation. On May 6, 2020, the investigation revealed that the personal information of certain FOI patients may have been accessed or taken during the incident. While we are not aware of the misuse of any information impacted by this incident, we are sending you this letter to notify you about the incident and provide information about steps you can take to help protect your information.

What Information Was Involved? Based on our investigation, your name, date of birth, Social Security number, medical information related to appointment times, physician locations, diagnosis codes, and payment amounts, insurance plan identification number, payer identification number, claims address, and/or FOI claims history may have been impacted by this incident.

What We Are Doing. As soon as we discovered the incident, we took the steps discussed above. To help relieve concerns and protect your identity following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit [https://\[IDMonitoringURL\]](https://[IDMonitoringURL]) to activate and take advantage of your identity monitoring services.

You have until [Date] to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

What You Can Do. We encourage you to contact Kroll with any questions by calling 1-???-???-?????. The call center is available Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. Please note the deadline to enroll is <<Date>>.

Again, at this time, while there is no evidence that your information has been misused, we encourage you to take full advantage of this service offering. Kroll representatives are available to answer questions or concerns you may have regarding protection of your personal information.

For More Information. If you have questions or need assistance, please call 1-???-???-????, Monday through Friday from 9 a.m. to 6:30 p.m. Eastern Time. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Chris Patterson". The signature is fluid and cursive, with the first name "Chris" being more prominent than the last name "Patterson".

Chris Patterson
HIPAA Security Officer
Florida Orthopaedic Institute

Steps You Can Take to Further Help 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 P.O. Box 1000 Chester, PA 19016 1-800-909-8872 www.transunion.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-685-1111 www.equifax.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.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 at least one 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: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. 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. 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 fraud alerts, security freezes, and 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. Contact information for the FTC is: Federal Trade Commission, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov and www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General Bureau of Internet and Technology Resources 28 Liberty Street New York, NY 10005 ifraud@ag.ny.gov 1-212-416-8433	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 www.oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 www.ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 www.riag.ri.gov 401-274-4400
---	---	---	---

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.