Central Kansas Orthopedic Group

SURGICAL SPECIALISTS & PHYSICAL THERAPY

February 6, 2020

VIA FIRST CLASS U.S. MAIL

Attorney General Gordon MacDonald
NH Department of Justice
33 Capitol Street
Concord, NH 03301

Dear Attorney General MacDonald:

Pursuant to (N.H. RSA §§ 359-C:20(I)(b) and 358-A:3(I)), we are writing on behalf of Central Kansas Orthopedic Group, P.C. ("CKO") to notify you of a breach of security involving one (1) New Hampshire residents. Beginning on November 11 of 2019, an unauthorized party or group (the "attacker") began to encrypt certain files within CKO's network environment (the "ransomware incident"). Some of the encrypted information included patient records. CKO did not pay the ransom and was able to restore its network environment from available backups.

Shortly after the ransomware incident, CKO sought outside legal counsel, who in turn immediately hired a third-party forensic investigator. Based upon the initial findings, we had no factual basis to assume that patient records had been accessed by the attacker – only that the servers on which the patient records were stored had been encrypted. Approximately one month after the investigation began however, however, the forensic investigator determined that the attacker had likely compromised an administrator account within the environment and exploited that account both to import a variety of software tools prior to the ransomware incident and to access servers containing patient records. The forensic investigation also found evidence of at least one incident in which the attacker exfiltrated an unknown data set from the environment. Based on the contents of the servers the attacker accessed, we cannot rule out the possibility that the attacker exfiltrated patient records. We have received no indication that any personal information has actually been misused in any way since the ransomware incident. The patient records included the following information:

1) Name
2) Address

3) Date of Birth
4) Driver's License Number (or other form of state-issued identification)
5) Health information related to your treatment at CKO or referring providers
6) Health insurance number
7) Social Security Number
8) Email address

CKO has already implemented the majority of its forensic investigators' recommendations, to harden our systems against future attacks of this kind and improve our information security, and will fully comply with those recommendations shortly. We have also informed law enforcement of this incident and will cooperate fully with any investigation by them or any regulatory body with oversight authority over this matter.

The affected patients, including the New Hampshire resident mentioned above, are receiving a written, mailed notice in connection with CKO's Health Information Portability and Accountability Act of 1996 ("HIPAA") responsibilities, specifically the HIPAA breach notification rule (45 C.F.R. Chapter 164, Part D), and as required by (N.H. RSA §§ 359-C:20(I)(b) and 358-A:3(I).). A sample copy of that notice is attached hereto.

CKO is offering identity theft protection services through ID Experts, which includes 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. CKO is also offering a call center to affected individuals.

CKO regrets this incident and is committed to its patients' privacy. If you have any questions about this matter, please contact my legal counsel, Todd Kinney, at (402) 346-6000 or todd.kinney@kutakrock.com.

Sincerely,

Leonard T. Fleske, M.D.
Owner, Central Kansas Orthopedic Group

Randall K. Hildebrand, M.D.
Owner, Central Kansas Orthopedic Group

Enclosure
cc: Todd Kinney, Esq.

Central Kansas
Orthopedic Group
SURGICAL SPECIALISTS & PHYSICAL THERAPY

C/O ID Experts
PO Box 4219
Everett, WA 98204

To Enroll, Please Call:
(833) 719-0128
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

F2698-1KS-0000001 P001 T00001 *********ALL FOR **** ###
<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

January 23, 2020

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

We are writing to make you aware of a privacy issue that took place at Central Kansas Orthopedic Group ("CKOG"). We take the privacy of our patients very seriously and understand that your personal information is important to you.

What Happened

On November 11, 2019, CKOG discovered that someone hacked its system when the intruder deployed ransomware. CKOG did not pay the ransom and was able to restore its system from available backups. The unauthorized access was shut down immediately upon CKOG discovering it. All medical records were restored. While we have no indication that any of your personal information has been misused in any way since the attack, it is possible that an unauthorized person or persons viewed your medical records.

What Information Was Involved

The information that may have been accessed by the hacker includes:

1) Name
2) Address
3) Date of birth
4) Driver's license number (or other form of state-issued identification)
5) Health information related to treatment at CKOG or referring physicians
6) Health insurance number
7) Social security number
8) Email address

What We Did and What We Are Doing

When CKOG discovered the ransomware attack, it immediately engaged outside counsel and a third-party forensic investigator to determine the scope and cause of the breach. We also notified law enforcement. We took immediate steps to increase security that assisted in shutting down access by the attacker. After a full forensic investigation, CKOG has no evidence to suggest that any personal information was removed from its system by any third party (including the attacker).

We take our responsibility to safeguard your personal information seriously and will comply with our forensic investigator's recommendations to further harden our systems against future attacks of this kind and improve our information security. We will cooperate fully with any investigation by law enforcement or any regulatory body with oversight authority over this matter.

In the interest of protecting our patients, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact ID Experts to enroll in free MyIDCare services by calling (833) 719-0128 or going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is April 23, 2020.

We encourage you to take full advantage of this service offering and reach out to CKOG with any questions and concerns.

There are additional actions you can consider taking to reduce the risk of identity theft or fraud on your account(s). Please refer to the enclosed Recommended Steps document for more information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call (833) 719-0128 or go to https://app.myidcare.com/account-creation/protect for assistance with any additional questions you may have about enrolling in MyIDCare services.

If you have any questions about the underlying incident, please feel free to call (833) 719-0128.

Sincerely,

Leonard T. Fleske, M.D.
Owner, Central Kansas Orthopedic Group

Randall K. Hildebrand, M.D.
Owner, Central Kansas Orthopedic Group

(Enclosure)

MyIDCare

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at (833) 719-0128 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

0000001

F2698-L01

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: Office of the Attorney General of New York, Bureau of Internet and Technology, 28 Liberty Street, New York, NY 10005, https://ag.ny.gov/bureau/internet-bureau, Phone: (212) 416-8433.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.