

CLARK HILL

Melissa K. Ventrone
T 312.360.2506
F 312.517.7572
Email: mventrone@clarkhill.com

Clark Hill
130 East Randolph Street
Suite 3900
Chicago, IL 60601
T 312.985.5900
F 312.985.5999

clarkhill.com

May 15, 2020

Via attorneygeneral@doj.nh.gov
Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Dear Attorney General Gordon MacDonald:

We represent Mat-Su Surgical Associates, APC (“MSA”) with respect to a data security incident involving the potential exposure of certain personally identifiable information described in more detail below. MSA, located in Palmer, Alaska, administers surgical procedures care to its patients. MSA is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On March 16, 2020, MSA suffered a cyber-attack known as ransomware that encrypted files on their system. MSA restored its systems, and there was no interruption of service to patients. Additionally, MSA began an internal investigation and hired independent computer forensic investigators to help determine what occurred, and whether any information was at risk. The forensic investigators found that an unauthorized actor gained access to files stored on MSA’s system that may have contained protected health information (“PHI”). Unfortunately, the investigators were unable to identify all files that may have been viewed by the unauthorized actor. Information that may have been impacted as a result of this incident includes patient names, addresses, Social Security numbers, diagnosis and treatment information, test results, health insurance information, and other information related to patient’s medical care.

2. Number of residents affected.

Four (4) New Hampshire residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on May 15, 2020 via regular mail (a copy of the form notification letter is enclosed).

3. Steps taken relating to the incident.

May 15, 2020

Page 2

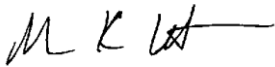
Since the incident, MSA has taken steps to minimize the risk of this kind of event from happening in the future, including resetting all passwords and putting additional controls in place for any type of remote access. MSA is also reviewing its policies and procedures to ensure that the appropriate controls are in place to protect PHI.

4. Contact information.

MSA takes the security of the information in its control seriously and is committed to ensuring the information in its control is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Very truly yours,

CLARK HILL

A handwritten signature in black ink, appearing to read "M K Ventrone", with a long horizontal flourish extending to the right.

Melissa K. Ventrone
Partner

(Enclosure)



C/O ID Experts

<<Return Address>>

<<City>>, <<State>> <<Zip>>

<<First Name>> <<Last Name>>

<<Address1>> <<Address2>>

<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
(833) 579-1096
Or Visit:
<https://app.myidcare.com/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

May 15, 2020

Notice of Data Breach

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

We are writing to inform you of a data security incident experienced by Mat-Su Surgical Associates, APC (“MSA”) that may have impacted your protected health information (“PHI”), including your name and Social Security number. MSA may have your information if you are a current or former patient of MSA or Valley Surgical Associates. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

What happened:

On March 16, 2020, we suffered a cyber-attack known as ransomware that encrypted files on our system. We immediately began an internal investigation and hired independent computer forensic investigators to help us determine what occurred, and whether any information was at risk. The forensic investigators found that an unauthorized actor gained access to files stored on our system that may have contained some of your PHI. Unfortunately, the investigators were unable to identify all files that may have been viewed by the unauthorized actor.

What information was involved:

From our investigation, it appears that documents stored on our system may have contained your name, address, Social Security number, diagnosis and treatment information, test results, health insurance information, and other information related to your medical care.

What we are doing:

We want to assure you that we are taking steps to minimize the risk of this kind of event from happening in the future. Since the incident, we have put additional controls in place for any type of remote access to our systems and implemented a global password reset. We are also reviewing our policies and procedures to ensure that the appropriate controls are in place to protect PHI. We have also arranged for you to receive credit monitoring and identity protection services at no cost to you.

What you can do:

MSA values you and the security of your personal information. We have arranged for you to receive credit monitoring identity protection services provided by MyIDCare™ powered by ID Experts. 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.

How to Enroll: You can sign up online or via telephone

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (833) 579-1096 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 5 am - 5 pm Alaska Time. Please note the deadline to enroll is August 15, 2020.

For more information:

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, 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) 579-1096 or go to <https://app.myidcare.com/account-creation/protect> for assistance or for any additional questions you may have.

Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,



Garth W. LeCheminant, M.D.
Owner
Mat-Su Surgical Associates, APC



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) 579-1096 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
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.alerts.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
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.

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 (<http://www.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.

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

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

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.