LEWIS BRISBOIS BISGAARD & SMITH LLP

Bryan M. Thompson
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
Bryan.Thompson@lewisbrisbois.com
Direct: 971.334.7009

August 29, 2020

File No. 48650.02

VIA E-MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
E-Mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Glacier Surgical Associates, Shannon Gulley, M.D. FACS, and Glacier Med Spa (collectively "Glacier Medical Group"), located in Palmer, Alaska. This letter is being sent in regards to a data security event involving Mat-Su Surgical Associates, APC ("Mat-Su Surgical"), a facility in Palmer, Alaska, where Dr. Shannon Gulley treated patients previously, which may have affected the information of one (1) New Hampshire resident.

1. **Nature of the data security incident.**

On March 16, 2020, Mat-Su Surgical suffered a ransomware incident that encrypted files on Mat-Su Surgical's systems, including patient information. Mat-Su Surgical's investigation found that an unauthorized actor gained access to and viewed files stored on Mat-Su Surgical's systems. Dr. Gulley treated individuals at Mat-Su Surgical from 2014 to 2018, and Mat-Su believed that information of patients treated by Dr. Gulley when she was affiliated with Mat-Su Surgical was stored on an affected server at the time of the ransomware event.

On August 3, 2020, after requests for information about the incident, Mat-Su Surgical provided Glacier Medical Group a list of potentially impacted patients that were seen by Dr. Gulley while affiliated with Mat-Su Surgical. After receiving this list from Mat-Su Surgical, Glacier Medical Group worked to provide notice to all identifiable individuals as swiftly as possible. On August 25, 2020, Glacier Medical Group notified those impacted patients with valid address information via notification letter in accordance with HIPAA.

This event occurred entirely on Mat-Su Surgical's systems, was not the result of any action by Glacier Medical Group, and did not affect the security or integrity of any Glacier Medical Group systems.

2. Number of New Hampshire residents affected.

Glacier Medical Group ultimately identified one (1) New Hampshire resident whose information may have been impacted by the incident involving Mat-Su Surgical. The information potentially affected could include individuals' names, dates of birth, driver's license or personal identification card numbers, Social Security Numbers, medical information and history, diagnosis and treatment information, health insurance information and other information they provided related to their medical care.

3. Steps taken related to the incident.

As noted above, Glacier Medical Group is providing notice in accordance with HIPAA to those individuals that Mat-Su Surgical identified as patients of Dr. Gulley whose information may have been impacted by the ransomware event at Mat-Su Surgical. While the incident was not caused by any action of Glacier Medical Group and did not affect any Glacier Medical Group system, Glacier Medical Group is providing twelve (12) months of complimentary identity monitoring to the notified resident.

4. Contact information.

Please contact me at 971.334.7009 or via email at bryan.thompson@lewisbrisbois.com if you have any questions.

Very Respectfully,

Bryan M. Thompson of
LEWIS BRISBOIS BISGAARD & SMITH LLP

BMT:FC
Encl.: Consumer Notification Letter Template

GLACIER
SURGICAL ASSOCIATES

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: <<XXXXXXX>>

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Re: Notice of Data Security Incident

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

I am writing to inform you of a data security incident experienced by Mat-Su Surgical Associates, APC ("Mat-Su Surgical"), a facility where I treated patients previously, that may have involved your personal information. At Glacier Surgical Associates and Glacier Med Spa (collectively "Glacier Medical Group"), we take the privacy and security of its patient's information very seriously. This is why I am notifying you of the incident, offering you identity monitoring services, and informing you about steps you can take to help protect your personal information.

What Happened? On March 16, 2020, Mat-Su Surgical suffered a ransomware event that encrypted files on its systems. Mat-Su Surgical conducted an investigation and hired independent computer forensic investigators to help determine what occurred. Mat-Su Surgical's investigation found that an unauthorized actor gained access to and viewed files stored on Mat-Su Surgical's systems.

Following their investigation, Mat-Su Surgical informed Glacier Medical Group of the ransomware event that affected their systems, and that the information of my patients whom I saw while at their facilities was still stored on their systems at the time of the incident. Consequently, those individuals' information may also have been impacted by this incident. On August 3, 2020, Mat-Su Surgical provided a list of those individuals whom I treated while at Mat-Su Surgical and whose information may have been impacted. After reviewing this list, it appears that your information may have been involved in the incident affecting Mat-Su Surgical.

Please note this incident affected Mat-Su Surgical's systems, and was not the result of any action by Glacier Medical Group and did not affect the security or integrity of any Glacier Medical Group systems.

What Information Was Involved? The information involved is any information you provided to any staff member or healthcare professional at Mat-Su Surgical from September 1, 2014 - April 2, 2018, and may include your name, date of birth, drivers license or personal identification card number, Social Security Number, medical information and history, diagnosis and treatment information, health insurance information, and other information related to your medical care.

What Are We Doing? As soon as I discovered the incident, I took the steps described above. In addition, I am providing you with information about steps you can take to help protect your personal information, and offering free identity monitoring and recovery services for <<Product Duration>> months through ID Experts as described below.

What You Can Do: You can follow the recommendations included with this letter to protect your personal information. I strongly encourage you to enroll in the identity monitoring services I am offering through ID Experts to protect your personal information. To enroll, please visit https://app.myidcare.com/account-creation/protect or call 1-800-939-4170 and provide your enrollment code found above. Your <<Product Duration>> months of services will include credit monitoring, CyberScan dark web monitoring, identity theft insurance, and fully managed identity recovery services.

To receive credit services, you must be over the age of 18, and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. Additional information describing your services is included with this letter.

Please note you must enroll by <<Enrollment Deadline>>. If you have questions or need assistance, please call ID Experts at 1-800-939-4170.

For More Information: If you have any questions about this letter, please call 1-800-939-4170 Monday through Friday from 6 am - 5 pm Pacific Time. Please accept my sincere apologies and know that I deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Shannon Gulley, M.D., FACS
Glacier Medical Group

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, PA19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-909-8872	1-888-397-3742	1-800-685-1111	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	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 90 days. 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	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
28 Liberty Street	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
New York, NY 10005	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
ifraud@ag.ny.gov	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
1-212-416-8433	1-888-743-0023	1-877-566-7226	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