



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

FEB 22 2022

CONSUMER PROTECTION

Gregory Lederman
Office: (267) 930-4637
Fax: (267) 930-4771
Email: glederman@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 17, 2022

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Hofmann Arthritis Institute PLLC and Hofmann Arthritis Institute of Nevada PLLC (collectively "HAI"), located at 24 1100 E #101, Salt Lake City, UT 84102, and are writing to notify your Office of an incident that may affect the security of information relating to one (1) New Hampshire resident. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, HAI does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On November 15, 2021, HAI discovered that it was no longer able to access certain information being hosted by one of its third-party vendors, Alta Medical Management and ECL Group, LLC (collectively "AMM"). HAI immediately commenced an investigation and gathered information from AMM in order to determine the nature and scope of the issue. Through this investigation, HAI confirmed that the incident did not involve any internal HAI systems. While AMM did not provide details surrounding this issue, HAI's investigation determined on or about December 7, 2021 the inaccessibility of data was related to a cyber incident that occurred at AMM. Although HAI's investigation remains ongoing, to date HAI has not been able to determine whether patient information was accessed or taken as a result of the AMM incident. Therefore, out of an abundance of caution, HAI performed a comprehensive review to identify and provide notification of the incident to HAI patients whose information was potentially affected.

Although the information varies for each individual, the information that could have been subject to unauthorized access includes name, address, address, Social Security number, date of birth, driver's license number, financial information, medical information and/or health insurance and billing information.

Mullen.law

Notice to New Hampshire Resident

On or about February 4, 2022, HAI began providing notice of this incident to affected individuals. On or about February 17, 2022, HAI provided written notice to additional affected individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, HAI moved quickly to investigate and respond to the incident, assess the security of HAI systems, and notify potentially affected individuals. HAI is also working to review existing policies and procedures regarding its third-party vendors and working to evaluate additional measures and safeguards to protect against this type of incident in the future.

Additionally, HAI is providing complimentary access to credit monitoring services for one (1) year through IDX to individuals whose information was potentially affected by this incident. HAI is also providing impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4637.

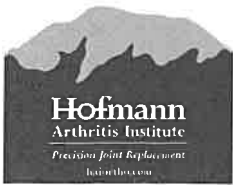
Very truly yours,



Gregory Lederman of
MULLEN COUGHLIN LLC

GCL/jlt
Enclosure

EXHIBIT A



P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-783-1442
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: [XXXXXXXXXX]

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

February 17, 2022

Re: Notice of <<Security Incident/Data Breach>>

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

Hofmann Arthritis Institute PLLC and Hofmann Arthritis Institute of Nevada PLLC (collectively “HAI”) is writing to inform you of a recent incident that occurred at one of our third-party vendors, Alta Medical Management and ECL Group, LLC (collectively “AMM”), which may impact the privacy of some of your information. AMM provides HAI with patient billing and accounting services to our patients. We are writing to provide you with information about the AMM incident, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it appropriate to do so.

What Happened? On November 15, 2021, HAI discovered that it was no longer able to access certain information hosted on AMM’s systems. HAI immediately commenced an investigation and gathered information from AMM in order to determine the nature and scope of the issue. Through this investigation, HAI confirmed that the incident did *not* involve any internal HAI systems, nor did it impact HAI’s electronic health records systems. While AMM did not provide details surrounding this issue, our investigation determined on or about December 7, 2021, the incident was related to a cyber incident that occurred at AMM.

What Information Was Involved? Although HAI’s investigation remains ongoing, to date we have not been able to determine whether patient information was accessed or taken as a result of the AMM incident. Therefore, out of an abundance of caution, HAI performed a comprehensive review to identify and provide notification of the incident to HAI patients whose information was potentially affected. This review was completed on January 27, 2022 and determined the following types of information related to you were potentially impacted by the AMM incident: your name, address, Social Security number, date of birth, driver’s license number, financial information, medical information and/or health insurance and billing information. To date, AMM has not reported to HAI that this information has been subject to actual or attempted misuse in relation to this incident.

What We Are Doing. HAI takes this incident and the security of information within our care very seriously. Upon discovery of this incident, we immediately launched an in-depth investigation to determine the full nature and scope of this incident. As part of our ongoing commitment to the privacy of information in our care, we are reviewing existing security policies and procedures regarding our third-party vendors and are working to evaluate additional measures to further protect against similar incidents moving forward. We will also be notifying state and federal regulators, as required.

In addition, we are offering identity theft protection services through IDX. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services, should you wish to enroll in these services. Please note the deadline to enroll is May 17, 2022.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your accounts statements and Explanation of Benefits reports, and to monitor your credit reports for suspicious activity and to detect errors. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Help Protect Your Information*. There, you will also find detailed instructions for credit monitoring enrollment. 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.

For More Information. We understand that you may have questions about the AMM incident that are not addressed in this letter. Please call 1-833-783-1442 Monday through Friday from 7 a.m. to 7 p.m. Mountain Time or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

HAI sincerely regrets any inconvenience or concern this incident may have caused you.

Sincerely,

Hofmann Arthritis Institute Management

Steps You Can Take to Help Protect Your Information

Enroll in Credit Monitoring

1. Website and Enrollment. Go to <https://app.idx.us/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 IDX identity protection 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, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-783-1442 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 IDX identity protection, notify them immediately by calling or by logging into the IDX 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. date of birth;
4. addresses for the prior two to five years;
5. proof of current address, such as a current utility bill or telephone bill;
6. a legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.); and

7. a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For 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 bureaus 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 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. We encourage you to 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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.