309 Fellowship Road, Suite 200
Mt. Laurel, NJ 08054

December 12, 2023

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Health Diagnostic Management, LLC ("HDM") located at 110 Marcus Drive, Melville, NY 11747, and are writing to notify your office of an incident that may affect the security of certain personal information relating to two (2) New Hampshire residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, HDM 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 or about October 13, 2023, HDM, which provides non-medical management services for diagnostic imaging centers, was made aware by their vendor, which operates HDM's patient portal, that there was suspicious activity on their patient portal, which is utilized by a number of HDM's customers and their patients. The vendor immediately launched an investigation and determined that an account associated with a referring physician with valid login credentials was engaged in unusual activity. Further investigation revealed that the referring physician, Brooklyn Premiere Orthopedics, announced a data breach a week prior to that unusual activity, leading to the conclusion that an unauthorized actor gained access to the patient portal and was able to access certain information held on that platform, and potentially to certain data, on October 12, 2023.

Following this determination, HDM's vendor and HDM began an in-depth process to identify the individuals whose information may have been impacted and reviewed internal HDM records to identify address information for potentially impacted individuals. This process concluded on November 21, 2023. As HDM is not the owner of the affected data, HDM began notifying its affected customers who are the owners of the data on October 16, 2023.

Notice to New Hampshire Residents

On or about December 12, 2023, HDM provided written notice of this incident to two (2) New Hampshire residents on behalf of the affected data owners. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. HDM is notifying on behalf of the affected data owners listed in ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon discovering the event, HDM moved quickly to investigate and respond to the incident, assess the security of HDM's patient portal, and identify potentially affected data owners and individuals. HDM is in the process of reviewing and implementing new security safeguards. HDM's vendor has engaged a third-party penetration testing firm to perform penetration testing on HDM's patient portal after making security updates. HDM is providing access to credit monitoring services for , through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, HDM is providing impacted individuals with guidance on how to better protect against identity theft and fraud. HDM is providing individuals with 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.

HDM is providing written notice of this incident to relevant state and federal regulators, as necessary. HDM is also notifying the U.S. Department of Health and Human Services.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at .

VFR/klh
Enclosure

EXHIBIT A

[Extra1]

Return Mail Processing
PO Box 999
Suwanee, GA 30024

11 1 1863 **********SNGLP
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

December 12, 2023

NOTICE OF DATA PRIVACY EVENT

Dear Sample A. Sample:

[Extra1] ("[Extra2]") is writing to make you aware of an incident that may affect the security of some of your personal information. Safeguarding information is among [Extra2]'s highest priorities, and this letter provides details of the incident, our response to it, and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or about October 13, 2023, [Extra2]'s third-party management company, which provides non-medical management services for diagnostic imaging centers, was made aware by their vendor that there was suspicious activity on their patient portal which [Extra2] utilizes. The patient portal allows for the uploading and viewing of MRI images, maintains patient information, medical information, scheduling access, and payment. The vendor immediately launched an investigation and determined an unauthorized actor gained access to the patient portal and was able to access certain information held on that platform, and potentially to certain data, on October 12, 2023.

Following this determination, the vendor, our third-party management company, and [Extra2] began an in-depth process to identify the individuals whose information may have been impacted, and reviewed internal [Extra2] records to identify address information for potentially impacted individuals. This process concluded on November 21, 2023. [Extra2] is notifying you out of an abundance of caution because the investigation determined that certain information relating to you may have been accessed or acquired by an unknown unauthorized person.

What Information Was Involved? Our investigation determined certain limited information was accessed without authorization. This information may include your name and [Extra3][Extra4]. [Extra2] is not aware of any attempted or actual misuse of your information.

What We Are Doing. Upon becoming aware of this incident, the vendor immediately took steps to confirm the security of the patient portal. We are reviewing existing security policies and the vendor implemented additional cybersecurity measures to further protect against similar incidents moving forward. We are notifying potentially impacted individuals, including you, so that you may take steps to best protect your information, should you feel it is appropriate to do so. We are also reporting to regulatory authorities, as required.

As an added precaution, we are offering you immediate access to credit monitoring and identity theft protection services for at no cost to you, through Experian. We encourage you to enroll in these services as we are not able to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed "*Steps You Can Take to Help Protect Your Information."*

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call 833-671-0081, Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays). We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

[Extra1]

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for .

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at . Be prepared to provide engagement number as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 1-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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 2 Rhode Island resident that may be impacted by this event.

EXHIBIT B