

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

October 30, 2023

VIA EMAIL (Idtheft@oag.state.md.us)

Brian E. Frosh
Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Northern Iowa Therapy – Incident Notification

To Whom it May Concern:

McDonald Hopkins PLC represents Northern Iowa Therapy PC (“NIT”). I am writing to provide notification of an incident at NIT that may affect the security of personal information of approximately one (1) Maryland resident. NIT’s investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, NIT does not waive any rights or defenses regarding the applicability of Virginia law or personal jurisdiction.

On March 10, 2023, NIT learned that a limited number of records were contained in an account unaffiliated with NIT. This did NOT include any access to our Electronic Medical Record system or payroll system. Upon learning of the issue, NIT commenced an immediate and thorough investigation. As part of its investigation, NIT engaged third-party experts experienced in handling these types of incidents. On June 21, 2023, NIT posted notice on its website alerting individuals of this incident. After an extensive forensic investigation and manual document review, we discovered on October 4, 2023 that the NIT records in the unaffiliated account may have contained some information of one Maryland resident including full name, Social Security number and driver’s license number.

NIT wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. NIT is providing the affected resident with written notification of this incident commencing on or about October 30, 2023 in substantially the same form as the letter attached hereto. NIT is offering the resident complimentary one-year membership with a credit monitoring service. NIT will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. NIT will advise the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free

October 30, 2023

Page 2

credit reports. The affected resident are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission and the Maryland Attorney General.

At NIT, protecting the privacy of personal information is a top priority. NIT is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. NIT continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,



James J. Giszczak

Encl.

P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: [REDACTED]

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

***IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY***

Dear [REDACTED]

Northern Iowa Therapy PC ("NIT") is committed to protecting the privacy and security of personal information in its position. We are writing with important information regarding a data security incident that involved some of your information. We want to provide you with information about the incident, inform you about the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On March 10, 2023, NIT learned that a limited number of records were contained in an account unaffiliated with NIT. This did NOT include any access to our Electronic Medical Record system or payroll system.

What We Are Doing.

Upon learning of the issue, NIT commenced an immediate and thorough investigation. As part of its investigation, NIT engaged third-party experts experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, we discovered on October 4, 2023 that the NIT records in the unaffiliated account may have contained some of your personal information. Please note that this incident did not impact our electronic medical records.

What Information Was Involved.

We want to be clear, our Electronic Medical Record System was NOT accessed. Based on our comprehensive investigation and manual document review, we determined that the records may have contained your [REDACTED]
[REDACTED]

What You Can Do.

We have no evidence that any of your information has been misused. To protect you from potential misuse of your information, NIT is working with IDX to provide identity theft protection services. IDX, A ZeroFox Company, is a data security and recovery services expert. IDX identity protection 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, IDX will help you resolve issues if your identity is compromised. Please see the following pages for enrollment instructions.

This letter also provides other precautionary measures that you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. To the extent that it is helpful, we have also provided information on protecting your medical information on the following pages.

For More Information.

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 8:00 a.m. to 8:00 p.m. Central time.

Sincerely,

Northern Iowa Therapy PC
[REDACTED]

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12 Month Credit Monitoring.

1. Website and Enrollment. Scan the QR image or visit <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. The enrollment deadline is [REDACTED]

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 1-888-567-0271 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.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial one (1) year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion LLC

P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/credit-freeze>
(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-freeze/> (800) 349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze> (888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze> (888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

6. Protecting Your Medical Information.

As a general matter, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.