McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Dominic A. Paluzzi
Direct Dial: 248-220-1356
E-mail: dpaluzzi@mcdonaldhopkins.com

February 14, 2025

MAILED VIA U.S. FIRST CLASS MAIL

Rhode Island Office of the Attorney General
c/o Consumer Protection Division
150 South Main Street
Providence, RI 02903

Re: Restorix Health, Inc.– Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Restorix Health, Inc. ("Restorix"). I am writing to provide notification of an incident at Restorix that may affect the security of personal information of Rhode Island residents. Restorix has notified potentially affected individuals on behalf of Kent County Memorial Hospital located at 455 Toll Gate Rd., Warwick, RI 02886.

As part of its notification to impacted individuals, Restorix has notified 510 Rhode Island residents. Restorix provided the affected residents with written notification of this incident pursuant to the HIPAA Breach Notification Rule, 45 CFR § 164.4041, commencing on February 14, 2025, in substantially the same form as the letter attached hereto. By providing this notice, Restorix does not waive any rights or defenses regarding the applicability of Rhode Island law or personal jurisdiction.

Restorix learned that an unauthorized individual may have obtained access to an employee's email account between May 7, 2024 and May 29, 2024. Restorix immediately launched an investigation in consultation with external cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the email account and the security of the emails and attachments contained within it. Restorix devoted considerable time and effort to determine what information was contained in the affected email account. Based on its comprehensive investigation and document review, Restorix discovered on November 27, 2024 that the compromised email account contained a limited amount of personal information, including the affected residents' full names and one or more of the following: Date of Birth, Treatment Information/Diagnosis, Provider Name, MRN/ Patient ID, and Health Insurance Policy/Subscriber Number. Restorix advised the covered entities of this incident on December 18, 2024.

To date, Restorix is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Restorix wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Restorix is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

Dominic A. Paluzzi

Encl.

[redacted]

RestorixHealth®
Excellence in Wound Care

THE WOUND CARE SOLUTIONS COMPANY
Providing programs, services, products and education across the care continuum.

[redacted]

February 14, 2025

[redacted]

Dear [redacted]

We are writing with important information regarding a recent data security incident that may have involved some of your personal information. Restorix Health, Inc. ("Restorix") is a healthcare services company that provides wound care management services to hospitals, including [redacted] The privacy and security of the information we maintain is of the utmost importance to Restorix. We wanted to provide you with information about the incident, and to let you know that we continue to take significant measures to protect your information.

What Happened?

On or around May 30, 2024, Restorix learned that an unauthorized actor obtained access to a Restorix employee's email account.

What We Are Doing.

Upon learning of this issue, we secured the account and commenced a prompt and thorough investigation in consultation with external cybersecurity professionals who regularly investigate and analyze these types of incidents. After an extensive investigation and manual document review, we discovered on November 27, 2024 that some of your personal information was contained in the account that was subject to unauthorized access between May 7, 2024 and May 29, 2024. Restorix advised [redacted] of this incident on December 18, 2024.

What Information Was Involved?

The accessed email account contained some of your personal information, including your name and [redacted]. Your Social Security number was not contained within the accessed account.

What You Can Do.

We have no evidence that any of your information has been misused as a direct result of this incident. Provided in the "Other Important Information" portion of this letter are precautionary measures 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. In addition, if this letter indicates that your medical information was involved, we have included steps you can take to protect such information.

For More Information.

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

If you have any further questions regarding this incident, please contact our toll-free incident response line at 1-833-799-4480, Monday through Friday from 8 am to 8 pm Eastern Time, excluding holidays.

Sincerely,

Restorix Health, Inc.

Other Important Information

1. Placing a Fraud Alert on Your Credit File.

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 30348-5069
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
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. 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 30348-5788
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888)-298-0045

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.

3. 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.

4. 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.

5. **Protecting Your Medical Information.**

In the event that your medical information was included in the accessed account, we have no information to date indicating that it was or will be used for any unintended purposes. As a general matter, however, 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.

Rhode Island Residents: You have the right to obtain a police report if one was filed, or alternatively, you can file a police report. Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above. In order to request a security freeze, you may need to provide the following information: your full name (including middle initial as well as Jr., Sr., II, III, etc.); Social Security number; date of birth; complete address; prior addresses; proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.); and if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. When you place a security freeze on your credit report, within five (5) business days you will be provided with a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following: (1) the unique personal identification number or password provided by the consumer reporting agency; (2) proper identification to verify your identity; and (3) the proper information regarding the period of time for which the report shall be available to users of the credit report. There were 510 Rhode Island residents impacted.