Dear Office of the Attorney General:

Pursuant to N.H. Rev. Stat. Ann. § 359-C:20, this email serves as notification of a data breach that impacted 7 New Hampshire residents.

On August 3, 2022, Riverside Medical Group (RMG), part of Optum, discovered an information security issue affecting an independent legacy server at our clinic located at 745 Northfield Ave, West Orange, NJ 07052. The compromised server belonged to a provider who used it to maintain some of his patients' immunization records. After detailed forensics work, RMG determined that the data contained on the server may have involved patient health and/or personal information. We are unaware of any actual misuse of the information. However, we are providing notice to affected patients out of an abundance of caution, because their information was available on the server, and potential access or acquisition of the information before the server was locked down could not be definitively ruled out.

Upon discovery, we took prompt action to lock down and disable the impacted server. We also began an investigation to understand the scope of the incident, confirming that other RMG systems and servers were unaffected. In addition, we have established a toll-free hotline that affected individuals can call if they have any questions.

Based on our review, the information that was involved may have included patient name, date of birth, address, gender, phone number, email address, immunization records, dates of immunizations, provider information, health plan information including ID number, and in limited instances, Social Security number (1 of the 7 impacted NH residents). The incident did not involve disclosure of or access to driver's license numbers or any financial account information. Affected individuals will be notified by mail on September 30, 2022. A copy of each notification letter template is attached.

Optum takes this matter seriously and is committed to protecting the privacy and security of our patients' personal information. Should you have any questions, please feel free to contact me at the phone number or email address listed below.

Tracy L. Ewing, CIPP/US (she / her)
Associate General Counsel
Director | Privacy Investigations
tracy.ewing@optum.com
Phone: 702-240-8806

Optum

Riverside MEDICAL GROUP

Your family's complete medical home.

[Date]
[Patient Name]
[Address]
[City, State Zip]

NOTICE OF DATA BREACH

Dear [Patient Full Name]:

We are writing to let you know about a privacy issue involving some of your information.

What Happened

On August 3, 2022, Riverside Medical Group (RMG) discovered an information security issue affecting an independent, legacy server at our West Orange (NJ) clinic. The compromised server belonged to a provider who used it to maintain some of his patients' immunization records. After detailed forensics work, RMG determined that the data contained on the server may have involved your health or personal information. We are unaware of any actual misuse of your information; however, we are providing notice to you out of an abundance of caution, because your information was available on the server, and potential access or acquisition of the information, before the server was locked down, could not be definitively ruled out.

What Information Was Involved

Based on our review, the information that was involved may have included your name, date of birth, address, gender, phone number, email address, immunization records, dates of immunizations, provider information, health plan information including ID number, and in limited instances, Social Security number. The incident did not involve disclosure of or access to your driver's license number or any financial account information.

What We Are Doing

We deeply regret this incident and sincerely apologize for any inconvenience or concern it may cause. Upon discovery, we took prompt action to lock down and disable the impacted server. We also began an investigation to understand the scope of the incident, confirming that other RMG systems and servers were unaffected. In addition, we have established a toll-free hotline that you can call if you have any questions (8am to 5pm EST). The toll-free telephone number is 855-487-6060.

What You Can Do

Although we are unaware of any misuse of your information, as a precaution, we recommend that you regularly monitor account statements and the explanation of benefits statements that you receive to check for any unfamiliar health care services. If you do not regularly receive explanation of benefits statements, you may request that your health plan send you these statements following the provision of any health care services.

As a precaution to help you detect any possible misuse of your personal information, we are offering you free "LifeLock® Identity Theft Protection Services," which proactively protects your personal and

financial information and provides comprehensive recovery services if you become a victim of identity theft during your LifeLock membership. Details of your complimentary membership are enclosed along with instructions for registering for this service. The enclosed Reference Guide provides additional steps you may take to monitor and protect your credit and finances.

For More Information

We take the privacy and security of our members' and customers' information seriously. We are reinforcing our existing policies and practices and evaluating additional safeguards to help prevent a similar incident from occurring in the future. Please call the dedicated toll-free hotline listed above if you have additional questions or concerns. Again, please accept our apologies for any concern this matter has caused.

Sincerely,

Shelley Violette
Associate Director | Privacy
Riverside Medical Group

LifeLock

NortonLifeLock Identity Theft Protection Services

UnitedHealth Group has partnered with NortonLifeLock, an industry leader in identity theft protection, to offer you one year of LifeLock service at no cost to you. Your promotional code is only valid for you and one dependent.

Details on Your Complimentary LifeLock Identity Theft Protection Are Below. You can enroll in LifeLock service by **phone** or **online**. You have until **December 30, 2022** to sign up for your membership.

Instructions to Enroll **ADULTS (18+)** in LifeLock Standard™	***Guardians must enroll with minors*** Instructions to Enroll **MINORS (Under 18)** in LifeLock Junior™
Enroll by Telephone: 1. Call LifeLock at **1-800-899-0180**. LifeLock representatives are available 24 hours a day, 7 days a week, 365 days a year. 2. Give the LifeLock representative your promotional code: ***RMG503** 3. Give the LifeLock representative your LifeLock Member ID. Your LifeLock Member ID is your first and last name with no spaces (Ex. Anthony Smith would be anthonysmith).	***Enroll by Telephone:*** 1. Call LifeLock at **1-800-899-0180**. LifeLock representatives are available 24 hours a day, 7 days a week, 365 days a year. 2. Give the LifeLock representative your promotional code: ***RMG010** 3. Give the LifeLock representative your LifeLock Member ID. Your LifeLock Member ID is your first and last name with no spaces (Ex. Anthony Smith would be anthonysmith).
Enroll Online: 1. Go to www.LifeLock.com. 2. Click on the **Start Membership** box in the middle of the webpage. 3. You will be taken to another page where, below the FOUR protection plan boxes, you will see the **Promo Code** box. Enter the **Promo Code: *RMG503** and click the **Apply** button. 4. Enter your first and last name (no spaces) in the LifeLock **Member ID** box (Ex. Anthony Smith would be anthonysmith) and click **Apply**. Your complimentary offer is presented. Click the red "**START YOUR MEMBERSHIP"** button.	***Enroll Online:*** 1. Go to www.LifeLock.com. 2. Click on the **Start Membership** box in the middle of the webpage. 3. You will be taken to another page where, below the FOUR protection plan boxes, you will see the **Promo Code** box. Enter the **Promo Code: *RMG010** and click the **Apply** button. ***The same Member ID will be used to activate your dependent's coverage.*** 4. Enter your first and last name (no spaces) in the LifeLock **Member ID** box (Ex. Anthony Smith would be anthonysmith) and click **Apply**. Your complimentary offer is presented. Click the red "**START YOUR MEMBERSHIP"** button

Once you have completed the LifeLock enrollment process, the service will be in effect. You will receive a welcome email or letter from LifeLock confirming your enrollment has been processed, although your protection begins immediately. If you have questions about the services offered or enrollment in LifeLock identity theft protection, please call **1-800-899-0180.**

For Adults (18 and over) - Your **LifeLock Standard™** membership includes:

- ✓ LifeLock Identity Alert™ System†
- ✓ 24/7 Live Member Support
- ✓ Dark Web Monitoring**
- ✓ LifeLock Privacy Monitor™
- ✓ Lost Wallet Protection
- ✓ Stolen Funds Reimbursement up to $25,000 †††
- ✓ Personal Expense Compensation up to $25,000 †††
- ✓ Coverage for Lawyers and Experts up to $1 million †††
- ✓ U.S.-Based Identity Restoration Team
- ✓ One-Bureau Credit Monitoring[1]**
- ✓ Reduced Pre-Approved Credit Card Offers
- ✓ USPS Address Change Verification

[1] If your plan includes credit reports, scores, and/or credit monitoring features ("Credit Features"), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment.
No one can prevent all identity theft or cybercrime. † LifeLock does not monitor all transactions at all businesses.
** These features are not enabled upon enrollment. Member must take action to get their protection.
††† Reimbursement and Expense Compensation, each with limits of up to $25,000 for Standard. And up to $1 million for coverage for lawyers and experts if needed. Benefits under the Master Policy are issued and covered by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

For Minors (Under 18) - Your **LifeLock Junior™** membership includes:

- ✓ LifeLock Identity Alert™ System†
- ✓ Dark Web Monitoring
- ✓ Credit File Detection**
- ✓ Lost Wallet Protection**
- ✓ File-Sharing Network Searches**
- ✓ 24/7 Live Member Support
- ✓ U.S.-Based Identity Restoration Specialists
- ✓ Million Dollar Protection™ Package†††
- ✓ Stolen Funds Reimbursement up to $25,000
- ✓ Personal Expense Compensation up to $25,000
- ✓ Coverage for Lawyers and Experts up to $1Million

No one can prevent all identity theft or cybercrime. † LifeLock does not monitor all transactions at all businesses.
**These features are not enabled upon enrollment. Member must take action to get their protection.
†††Reimbursement and Expense Compensation, each with limits of up to $25,000 for Defender. And up to $1 million for coverage for lawyers and experts if needed. Benefits under the Master Policy are issued and covered by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

Reference Guide

Order Your Free Credit Report

You are entitled to receive your credit report from each of the three national credit reporting agencies once per year, free of charge. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free at 1-877-322-8228, or by mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually. They provide free annual credit reports only through the website or toll-free number.

When you receive your credit report(s), review them carefully. Look for any inaccurate information and contact the appropriate credit reporting agency to notify of any incorrect information, including accounts you did not open; requests for your credit report from anyone that you did not apply for credit with; or inaccuracies regarding your personal identifying information, such as your home address and Social Security number. If you find anything that you do not understand or that is incorrect, contact the appropriate credit reporting agency using the contact information on the credit report as soon as possible so the information can be investigated, and if found to be in error, corrected.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in your financial accounts, promptly notify your credit card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission. If you believe your identity has been stolen, the U.S. Federal Trade Commission ("FTC") has created a one-stop resource site that provides and interactive checklist that walks through the steps people need to take upon learning that their identity has been stolen or their personal information has been compromised in a data breach. The FTC recommends that you take these additional 4 steps right away when you become a victim:

Step 1: Call the companies where you know fraud occurred.

Step 2: Place a fraud alert and get your credit report.

Step 3: Report identity theft to the FTC.

Step 4: File a report with your local police department.

A checklist of the steps listed above and links to forms and other helpful information can be found on the site at IdentityTheft.gov/steps.

You can learn more about how to protect yourself from becoming a victim of identity theft by contacting the FTC at the address below or visiting the website below:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-438-4338
1-866-653-4261 (TTY)
http://www.consumer.ftc.gov/features/feature-0014-identity-theft

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Credit Agency	Mailing Address	Phone Number	Website
Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Fraud Request Form *Mail the fraud request form to the address listed above.	1-800-525-6285	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
Experian	Experian P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	https://fraud.transunion.com/

Place a Security Freeze on Your Credit File

You may wish to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. The credit bureaus may charge a reasonable fee to place a freeze on your account and may require that you provide proper identification prior to honoring your request. You can request a security freeze by contacting the credit bureaus at:

Credit Agency	Mailing Address*	Phone Number	Website
Equifax	Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 Equifax Freeze Request Form *Mail the freeze request form to the address listed above.	Automated line: 1-800-349-9960 Customer Care: 1-888-298-0045	https://www.equifax.com/personal/credit-report-services/credit-freeze//
Experian	Experian P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/freeze
TransUnion	TransUnion P.O. Box 160 Woodlyn, PA 19016	1-888-909-8872	https://www.transunion.com/credit-freeze

Additional Attorney General Office Identity Theft Resources. You can obtain information from your state's Attorney General's Office about steps that you can take to help prevent identify theft. Please see the information below for states that provide these resources:

For California Residents. You can obtain additional information from the California Department of Justice's Privacy Enforcement and Protection Unit (https://oag.ca.gov/privacy) to learn more about protection against identity theft.

For District of Columbia Residents. You can obtain additional identity theft information from the District of Columbia's Attorney General Office (https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft) to learn more about protection against identity theft.

For Maryland Residents. You can contact the Maryland Attorney General at:
Maryland Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
25th Floor
Baltimore, MD 21202

Phone: 1-410-576-6491
Fax: 1-410-576-6566
Email: idtheft@oag.state.md.us
Website: https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx

For North Carolina Residents You can contact the North Carolina Attorney General at:
North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
Phone: 1-877-566-7226 (Toll-free within North Carolina), 1-919-716-6000
Website: https://ncdoj.gov/
Identity Theft Link: Protecting Your Identity - ID Theft Protection by NC DOJ.

For Oregon Residents. You can obtain additional identity theft information from the Oregon Attorney General Office (https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/) to learn more about protection against identity theft.

For Rhode Island Residents. You can contact the Rhode Island Attorney General at:
Rhode Island Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
Phone: 1-401-274-4400
Fax: 1-401-462-9532
Email: DBR.Insurance@dbr.ri.gov
Website: http://www.riag.ri.gov/ConsumerProtection/About.php#

Precautions to Help You Avoid Becoming a Victim

1. Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues or any other internal information. If an unknown, individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

2. Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

3. Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

4. Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, http://www.us-cert.gov/ncas/tips/ST04-013).

5. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

6. If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is

also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).

7. Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (for more information, see Understanding Firewalls, http://www.us-cert.gov/ncas/tips/ST04-004; Understanding Anti-Virus Software, http://www.us-cert.gov/ncas/tips/ST04-005; and Reducing Spam, http://www.us-cert.gov/ncas/tips/ST04-007).

8. Take advantage of any anti-phishing features offered by your email client and web browser.

9. Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at www.ic3.gov.