WINSTON & STRAWN LLP

NORTH AMERICA SOUTH AMERICA EUROPE ASIA

35 W. Wacker Drive
Chicago, IL 60601
T +1 (312) 558-5600
F +1 (312) 558-5700

VIA OVERNIGHT MAIL

March 11, 2024

Attorney General John Formella
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, New Hampshire 03301

Re: Notice of Privacy Incident

To Whom It May Concern:

Winston & Strawn LLP ("Winston") represents R1 RCM Inc. ("R1"), 8750 W. Bryn Mawr Street, Suite 115, Chicago, Illinois, 60631, with respect to the privacy incident that is the subject of this letter (the "Privacy Incident"). R1 is providing this notification at the direction of St. Rose Dominican Hospital de Lima, a Dignity Health hospital ("Dignity"), as R1 is a "business associate" of Dignity, which is a "covered entity" as such terms are defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Privacy Incident potentially affected approximately two (2) individuals who had New Hampshire addresses on record with Dignity.

By way of background, on November 17, 2023, R1 became aware that protected health information ("PHI") associated with Dignity was in the possession of an unauthorized third party. R1 immediately began an investigation into the matter and determined that a copy of this PHI was present on a server when such server was targeted by the exploitation of a zero-day vulnerability of GoAnywhere software by the same unauthorized third party on January 30, 2023 (the "GoAnywhere Event"). While it could not be definitively confirmed that the GoAnywhere Event was the source of the PHI, this notice is being provided out of an abundance of caution.

R1 undertook an analysis of the Dignity PHI and on, January 11, 2024, determined that certain PHI, including

. Notification letters will be mailed to potentially impacted individuals on March 11, 2024. An example of the notification letter that will be sent to potentially impacted individuals in New Hampshire is included as Exhibit 1 to this letter.

Following the Privacy Incident, R1 rebuilt the impacted server and implemented the patch released by GoAnywhere designed to address the vulnerability at issue. In addition, out of an abundance of caution, R1 has secured the services of Kroll, Inc. to offer of identity monitoring services at no cost to the potentially impacted New Hampshire residents.

By providing the information in this letter, R1 expressly reserves all available rights, defenses, and privileges in connection with the Privacy Incident. Furthermore, R1 does not admit or concede any liability or wrongdoing, and expressly reserves its right to contest or challenge any findings or conclusions of any investigation by this office or any other office or agency with appropriate jurisdiction. Finally, this notice is not, and does not otherwise constitute, a waiver of R1's objection that New Hampshire lacks personal jurisdiction with respect to the Privacy Incident.

It is my hope that this letter will satisfy this office's need for information related to the Privacy Incident. However, if this office requires any additional details, please contact me by telephone at

Sincerely,

Alessandra V. Swanson

Attachment: Exhibit 1 – Example Notification Letter

EXHIBIT 1
Example Notification Letter

See attached.

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

R1 RCM Inc. ("R1") is providing this notice to you on behalf of St. Rose Dominican Hospital de Lima, a Dignity Health hospital ("Dignity") regarding an incident that may have impacted the privacy of your protected health information ("PHI"). R1 is contacting you because we are a business associate of Dignity and processed your PHI in the course of providing those services. This notice provides information about the incident, the actions we are taking out of an abundance of caution and what to do if you have further questions.

R1 became aware on November 17, 2023 that PHI associated with Dignity was in the possession of an unauthorized third party (the "Dignity PHI"). R1 immediately began an investigation into the matter and determined a copy of this PHI was present on a server maintained by CloudMed, an R1 company, when the server was targeted by the exploitation of a zero-day vulnerability of GoAnywhere software by the same unauthorized third party on January 30, 2023 (the "GoAnywhere Event"). While we could not definitively confirm that the GoAnywhere Event was the source of the PHI at issue, we are nonetheless providing this notice out of an abundance of caution.

R1 undertook an analysis of the Dignity PHI and on, January 11, 2024, determined that certain PHI, including your name, contact information, date of birth, Social Security number, location of services, clinical and/or diagnosis information and patient account and/or medical record number was potentially included in the Dignity PHI.

In connection with R1's response to the GoAnywhere Event, R1 rebuilt the impacted server and implemented the patch released by GoAnywhere in February 2023 designed to address the vulnerability at issue. In addition, out of an abundance of caution, we have secured the services of Kroll to provide two years of identity monitoring services at no cost to you. You can visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services. You have until **<<b2b_text_6 (activation date)>>** to activate your identity monitoring services. Your membership number is **<<Membership Number s_n>>**.

We encourage you to remain vigilant to the possibility of fraud by reviewing your account statements and monitoring free credit reports for any unauthorized activity and reporting any such activity. Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call (866) 495-4603, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

R1 RCM Inc.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are certain changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You will have access to a Kroll fraud specialist. Support includes showing you helpful ways to protect your identity, explaining your rights and protections under the law, providing assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to help resolve related issues. You will have access to an investigator who understands your issues and can help do the work for you. Your investigator will make efforts to uncover the scope of the identity theft and then help work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL RESOURCES

Review Account Statements and Credit Reports

We recommend you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, a consumer may be entitled every 12 months to one free copy of the consumer's 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. Consumers may wish to stagger their requests so that they receive free reports from one of the three credit bureaus every four months.

Place a Fraud Alert or Credit Freeze

A consumer can 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 displayed on a consumer's credit file, a business must verify the consumer's identity before extending new credit. Victims of identity theft may be entitled to an extended fraud alert, which is a fraud alert lasting seven years. To place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, a consumer has 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 the consumer's name without the consumer's consent. However, please be aware that using a credit freeze to control who can access a consumer's personal and financial information in the consumer's credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application the consumer makes regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, a consumer cannot be charged to place or lift a credit freeze on your credit report. The following information will need to be provided to request a credit freeze:

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 the consumer is a victim of identity theft.

To place a fraud alert or a 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

Other Steps You Can Take

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. In particular, the Federal Trade Commission encourages those who discover their information has been misused to file a complaint. You can obtain further information on filing such a complaint by using the contact information listed below.

You can file a police report in the event of identity theft or fraud. Please note that, to file a report with law enforcement for identity theft, you will likely need to provide some proof of the identity theft. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

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.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Massachusetts Residents: **You can file a police report in the event of identity theft or fraud.** Under Massachusetts law, you may have the right to file and obtain a copy of a police report. You may also have the right to request a security freeze, as described above. You may contact and obtain information from the Massachusetts Attorney General at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. Instances of known or suspected identity theft should also be reported to law enforcement and the Attorney General.