HORIZON
HEALTHCARE RCM

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

KROLL
SCAN TO ENROLL

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

<<b2b_text_1 (Extra 1) (Notice of Data Breach)>>

Dear <<First_name>> <<Last_name>>:

Horizon Healthcare RCM ("Horizon") writes to inform you about a matter that may involve your information, our response, and steps you may take should you feel it is appropriate to do so. Horizon is a former revenue-cycle management company that provided hospitals, health systems, and medical centers with accounts receivable and revenue reporting services. Horizon had your information because you received medical services from <<b2b_text_5 (Extra2) (CoveredEntity)>>, a former Horizon customer. Please note that this notice is limited to an issue that occurred on our systems. This issue does not involve or otherwise impact our former customer's systems or information they maintain about you on their systems.

What Happened? On December 27, 2024, we learned that a computer virus was used to lock access to some files stored on our computer network. In response, we securely restored our systems and took steps to determine what occurred. During our investigation of this matter, we identified that files on certain systems were likely copied without permission between December 26 and 27. To ensure we could properly notify patients whose information was in the copied files, including the types of information contained within the files, we undertook an intensive review of those files, which concluded, with respect to your information, on September 23, 2025. We updated our former customer at the end of September 2025 to obtain permission to notify patients, and we worked to gather updated contact information to send notices. With respect to the above-referenced former customer, their review of this matter was complete on <<b2b_text_4 (Extra3) (review completion date)>>.

What Information Was Involved? The files contained your name and the following types of information: <<b2b_text_2 (Extra4) (Data Elements) >>. Please note, however, that your information being contained in the files does not mean you are the victim of identity theft or fraud, and we have no indication of an individual experiencing verified identity theft as a result of this incident. Any steps you may wish to take in response to this matter are a personal decision. Nevertheless, if you have any concerns, we are providing you with complimentary identity monitoring and free resources detailed below.

What We Are Doing. We arranged for the party responsible for this matter to delete the copied information. Further, Horizon is providing notice of this event to individuals so they may take steps to help safeguard their information, should they feel it appropriate to do so. We are also providing free resources and guidance in the "Steps Individuals Can Take To Protect Personal Information" section below. While no safeguards can fully prevent all cybersecurity attacks, we also implemented additional technical measures and processes to further enhance the company's security.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your relevant account statements, if any, and monitoring your free credit reports for suspicious activity and to detect errors. We also recommend you review the "Steps Individuals Can Take To Protect Personal Information" section of this letter and enroll in the complimentary identity monitoring.

For More Information. If you have questions about this matter, please contact our toll-free assistance line at (866) 461-8271, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding U.S. holidays). You may also write to Horizon at Horizon Healthcare RCM, Attn: Compliance, 9980 Georgia St, Crown Point, IN 46307.

Sincerely,

Horizon Healthcare RCM

Steps Individuals Can Take To Protect Personal Information

Enroll in Monitoring Services

KROLL

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<ServiceTerminMonths>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

To enroll in the complimentary Kroll identity monitoring services, please follow the instructions below:

- Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
- You have until *<<b2b_text_6 (activation deadline)>>* to activate your identity monitoring services.
- Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your identity monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

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.

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/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, 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 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 Ave 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave NW, Washington, D.C. 20580.

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 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.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. <<b2b_text_3 (There are approximately [Number] Rhode Island residents that may be impacted by this event.) >>

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 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. 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.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, 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 resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.