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

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

Re: Notice of Data Breach

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

Healthcare Resource Group, Inc. ("HRG") is writing to notify you of a recent event that may impact the privacy of some of your personal information. HRG provides billing services to Barlow Respiratory Hospital ("Barlow") and had access to some of your information in connection with assisting Barlow with its referral process. Although we have no evidence of actual misuse of any of your information, we are notifying you out of an abundance of caution and providing you with steps you may take to help further protect your personal information.

What Happened? On December 31, 2019, as part of the investigation of an unrelated event, HRG determined that an employee's email account was subject to unauthorized access between November 4, 2019 and November 30, 2019. HRG was unable to determine what, if any, emails and attachments within the account were subject to unauthorized access. We were only able to confirm that the email account was subject to unauthorized access. HRG then enlisted the services of a third-party firm to review the contents of the email account in order to determine whether it contained any sensitive information. While the forensic investigation was ongoing, HRG initially notified Barlow of the event on February 6, 2020 and, at that time, stated it could not confirm whether any sensitive information was contained in the email account in question. HRG continued to conduct its forensic investigation and a time-intensive review of the email contents, which concluded on February 27, 2020. On March 11, 2020, HRG affirmatively notified Barlow about the findings from the forensic investigation and requested permission to provide you with notice on their behalf.

What Information Was Involved? After a thorough and exhaustive review process, HRG determined that the impacted email account contained the following types of information: your <<b2b_text_2(ImpactedData)>><<b2b_text_3(ImpactedData)>>. At this time, however, we have no evidence of actual misuse of any of your personal information.

What We Are Doing. Maintaining the privacy and security of your personal information is our highest priority. Upon learning of this incident, HRG immediately took steps to secure the email account and launched an in-depth investigation to determine the nature and scope of the incident. Law enforcement has also been notified. As part of HRG's ongoing commitment to the privacy of personal information in its care, HRG is currently evaluating and updating, as appropriate, its privacy policies and procedures. In addition, HRG has enhanced security awareness training among its workforce and implemented various additional technical safeguards to further secure the information in its systems. To help relieve concerns and restore confidence following this incident, we have arranged to offer you, at no cost to you, identity monitoring and identity theft consultation and restoration services through Kroll for 12 months. You may activate these services by following the instructions attached to this notice.

What You Can Do. Please review the enclosed "Steps You Can Take to Help Protect Your Information," which contains information on what you can do to better protect against possible misuse of your information. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity.

For More Information. We recognize that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call our toll-free dedicated assistance line at 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

We remain committed to safeguarding your information in our care and will continue to take steps to ensure the security of our systems.

Sincerely,

Kris Ditzler
Chief Financial Officer
Healthcare Resource Group, Inc.

Steps You Can Take to Help Protect Your Information

Activate Your Complimentary One-Year Identity Monitoring Service

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 one year. 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.

Visit **https://[IDMonitoringURL]** to activate and take advantage of your identity monitoring services.

You have until [Date] to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

Monitor Your Accounts/Credit Reports

You may obtain a copy of your credit report, free of charge, once every 12 months from each of the 3 nationwide credit reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Security Freeze

You have the right to place a "security freeze" on your credit report, free of charge. A security freeze will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact each of the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or up to 3 business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within 5 business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the 3 credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to remove the security freeze.

Fraud Alert

You also have the right to place an initial or extended "fraud alert" on your 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 displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. If you are a victim of identity theft and have filed an identity theft report with law enforcement, you may want to consider placing an extended fraud alert on your credit file. An extended fraud alert lasts for 7 years. Should you wish to place a fraud alert, please contact any of the 3 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC, proper law enforcement authorities, and/or your state attorney general. You may also contact these agencies, as well as consumer reporting agencies, for information on how to prevent or avoid identity theft and to obtain additional information about fraud alerts and security freezes.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For California Residents: You may also wish to review the information provided by the California Attorney General at https://oag.ca.gov/idtheft.

For 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, www.oag.state.md.us/Consumer, Telephone: (410) 576-6491.

For North Carolina residents: In addition to the FTC, you may obtain information about preventing identity theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourselffrom-id-theft, by writing to 9001 Mail Service Center, Raleigh, NC 27699-9001, or calling 1-877-566-7226 or 1-919-716-6000.

For New York residents: You may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General at https://ag.ny.gov/ or by calling 1-800-771-7755; the New York State Police at http://troopers.ny.gov/ or by calling 1-518-457-6721; and/or the New York Department of State at https://www.dos.ny.gov or by calling 1-800-697-1220.

For New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act ("FCRA"), such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the FCRA not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response 30-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at https://doj.state.or.us, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Protecting Your Health Information

We have no information to date indicating that your health information involved in this incident 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 with your medical care.*
- *Review your "explanation of benefits" statement which you can receive form 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 timeframe of the potential incident (noted above) to the 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.*

Kroll | A Division of DUFF & PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] 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 can help you determine if it's an indicator of identity theft.

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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] 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.