RC HOSPITAL & Clinics

[redacted]

[redacted]

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

<<Date>>

Dear [redacted]

The privacy of your personal information is of utmost importance to Renville County Hospital & Clinics. I am writing to provide you additional information about the tax fraud investigation and explain the additional services we are making available to help safeguard you against identity fraud.

As you know, Renville County Hospital & Clinics uses a third party vendor to provide W-2 and form 1095 documents to employees and process payroll. On April 13, 2016 Renville County Hospital & Clinics was notified that an unauthorized user accessed the vendor portal that stores the 2015 W-2, form 1095 and payroll information. The portal would allow access to data files which contain personal information of employees of Renville County Hospital & Clinics. Up to this point, our employees have not had access to this portal. After being notified of this issue, we have suspended any further upload of data to the vendor. In addition, we simultaneously commenced an investigation and engaged external cybersecurity professionals to analyze the extent of the compromise and assist in our response.

We are devoting considerable resources to identify exactly whose information may be at risk and contacting the potentially affected individuals. At this point in the investigation, it is unclear if your information was accessed. If your information was accessed, it would have contained your personal information, including your direct deposit information, which included your bank account number and routing information, as well as your 2015 W-2 which includes: your full name, address, and Social Security number. In addition, the file would have contained your form 1095, which includes your personal information, as set forth above, and your date of birth, and the personal information of your spouse and any dependents.

We are aware that some employees have received IRS discrepancy letters and/or have reported tax fraud issues - when they filed their tax return, the Internal Revenue Service rejected the filing, stating someone had already filed or attempted to file their tax return. At this time, we cannot say with certainty that these instances are directly related to this incident. Out of an abundance of caution, we wanted to make you aware of this incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps you should take.

Moreover, the information that may be at risk in this situation is the type of information that may be used to file fraudulent tax returns. As a result, you should contact your tax advisor, if you have one, and let them know this information may be at risk. You also should file your tax return as quickly as possible, if you have not done so.

If you believe you are a victim of identity fraud and it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax return electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended you: contact your tax preparer, if you have one; file an Identity Theft Affidavit (Form 14039) with the IRS (the form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf); call the IRS at (800) 908-4490, ext. 245 to report the situation (the unit office is open Monday through Friday from 7 am to 7 pm); and report the situation to the local police department. Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection.

Enclosed in this letter you will find information to enroll in a 1 year membership of Experian's ProtectMyID® Alert that we are providing at no cost to you. Other precautionary measures you can take to help protect your personal information include: placing a Fraud Alert and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis. Because your bank account number and routing information was accessed, we encourage you to talk with your bank regarding steps they suggest to protect your bank account.

Renville County Hospital & Clinics is committed to maintaining the privacy of our employees' information and has taken many precautions to help safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of our employees' information.

If you have any further questions regarding this incident, please call [redacted] during normal business hours.

Sincerely,

[redacted]

Renville County Hospital & Clinics

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary 1 Year Credit Monitoring.

Protecting your personal information is important to Renville County Hospital & Clinics. In response to this security incident and as a precautionary measure, we have arranged for you to enroll in Experian's® ProtectMyID® Alert for a one year period at no cost to you. This protection is provided by Experian, one of the three major nationwide credit reporting companies.

Activate Experian's® ProtectMyID Now in Three Easy Steps:

1. ENSURE that you enroll by [redacted]
2. VISIT the ProtectMyID Web Site to enroll: [redacted]
3. PROVIDE your 9-character Activation Code: [redacted]

If you have questions or need an alternative to enrolling online, please call [redacted] and provide Engagement [redacted]

Additional Details Regarding Your 1-Year ProtectMyID Membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after an incident. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers. (Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.)

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [redacted]

2. Security Freeze on Your Credit File.

If you are concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111

Experian Security Freeze
PO Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19022
http://www.transunion.com/securityfreeze
1-800-680-7289

3. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 1 year credit monitoring services, we recommend that you place an initial 90-day "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	**Experian**	**TransUnion**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

4. 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.

5. 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.

6. Reporting Identity Fraud to the IRS.

If you believe you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended you do the following:

- Contact your tax preparer, if you have one
- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf.
- Call the IRS at (800) 908-4490, ext 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm
- Report the situation to your local police or law enforcement department

Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection.

7. Reporting Identity Fraud to the Social Security Administration.

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount. For additional information, please see Identity Theft and Your Social Security Number at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

McDonald Hopkins

A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

METRO PLEX
MI 480
25 MAY '16
PM 1 L

Montana Attorney General
Office of Consumer Protection
P.O. Box 200151
Helena, Montana 59620

RECEIVED
MAY 31 2016
OFFICE OF CONSUMER PROTECTION

59620-015151