April 27, 2020

Dear [Employee Name],

NOTICE OF DATA BREACH

What Happened?	Marshall Medical Center (MMC) uses an outside vendor called PaperlessPay to produce electronic paystubs and W-2 forms for employees. On March 20, 2020 PaperlessPay contacted MMC that on February 19, 2020, the Department of Homeland Security ("DHS") contacted PaperlessPay that an unknown person was purporting to sell "access" to PaperlessPay's client database on the dark web. In response, PaperlessPay shut down its web server and database to prevent any potential unauthorized access. This interrupted services to MMC employees and prevented you from accessing payroll records for a short amount of time while the servers were offline. PaperlessPay does not have any role in the actual Direct Deposit process of paychecks, so that process was not impacted. Over the following weeks, PaperlessPay cooperated with the joint investigation conducted by DHS and the Federal Bureau of Investigation ("FBI"). Their investigation is ongoing, and PaperlessPay will continue to cooperate. In addition, PaperlessPay retained the cybersecurity firm Ankura to help with its own, internal forensic investigation of the incident. Through these investigations, PaperlessPay confirmed that an unknown person (the "Hacker") on February 18, 2020accessed PaperlessPay's database where MMC employees' data was stored. The available evidence has not, however, allowed DHS, the FBI, or Ankura to determine what data the Hacker may have accessed or viewed while connected to the database. It is possible the Hacker only used access to determine the size of the database and to stage it for subsequent access that could be sold to others, and that the Hacker did not directly access any employee data. The security system also has an alert system that is configured to detect data file transfers that exceed 1GB in size, and no alert was triggered during this security incident event. However, the Hacker would have had the capability to run queries against the database and view its data, so we cannot rule out the possibility of unauthorized access or acquisition.
What Information Was Involved?	The information stored in PaperlessPay's database regarding MMC employees consists of the data elements that appear on employee pay stubs and tax forms, including name, address, pay and withholdings, and Social Security number. However, these data elements are stored on the database in different tables that are associated by user ID numbers, not names, within each database table. Therefore, the only way to associate any data with an individual would be to run a query against the database and have it aggregate an individual's name with his or her other data components.

What We Are Doing.	PaperlessPay has acted to secure their network and prevent future incidents. To resume their services, PaperlessPay rebuilt a new domain controller, a new web server, and a new database server to start with a clean slate. Furthermore, PaperlessPay then restored database files to the new database server from backups. New IP addresses were assigned to all the new servers, and passwords for users and administrators were changed., These actions forced all clients to change their passwords when they login for the first time and disabled all remote access capabilities to the new web server and database server. PaperlessPay also installed an endpoint detection and response (EDR) application called Carbon Black on the new servers and other endpoints within its network. This has allowed PaperlessPay to monitor all activity while it completed its investigation of the incident. To date since Carbon Black has been running, there have been no indicators of compromise detected in the newly rebuilt environment, and PaperlessPay has reported that all customer services are functioning as normal. Based on the information PaperlessPay has shared with MMC about this event, MMC has decided to stop sending any more information to this vendor going forward. The previous data for e-stubs and W-2's will still be available through the PaperlessPay portal until we determine a better method for access. For a period of time, MMC will be going back to producing paper paystubs until we can go live on our new payroll system. MMC has purchased a new payroll system through a company called Workday and is building this system for go live this fall. The new payroll system will have an employee portal where employees will be able to access their paystubs and W-2 and will be included in the overall business system for the organization. To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. **Activate IdentityWorks Credit 3B Now in Three Easy Steps** **1.** ENROLL by: **7.21.2020** (Your code will not work after this date.) **2.** Visit the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit** **3.** PROVIDE the **Activation Code**: **[insert code]** If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number **DB19681** as proof of eligibility for the identity restoration services by Experian. **Additional details regarding your 12-MONTH EXPERIAN IDENTITYWORKS credit 3b Membership:** A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B. You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud. Once you enroll in Experian IdentityWorks, you will have access to the following additional features: • **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.* • **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.

	• **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired. • **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers. **Activate your membership today at https://www.experianidworks.com/3bcredit or call 877-288-8057 to register with the activation code above.**
What You Can Do.	There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). **ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT** ➢ **Place a 90-Day Fraud Alert on Your Credit file** An **initial 90-day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should takes steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance. **Equifax** 1-800-525-6285 www.equifax.com **Experian** 1-888-397-3742 www.experian.com **TransUnion** 1-800-680-7289 www.transunion.com ➢ **PLACE A SECURITY FREEZE ON YOUR CREDIT FILE** If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies. ➢ **Order Your Free Annual Credit Reports** Visit www.annualcreditreport.com or call 877-322-8228. 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. ➢ **MANAGE your personal information** Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information. ➢ **USE TOOLS FROM CREDIT PROVIDERS** Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

	➢ **Obtain more INFORMATION about identity theft and ways to protect yourself** • Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity. • The Federal Trade Commission has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.
We sincerely apologize for this incident, regret any inconvenience it may cause you and encourage you to take advantage of the product outlined herein.	
For More Information.	If you have any questions, please call the MMC payroll department at (530) 626-2866. We are here to help and support you through this process. Again, we apologize for any inconvenience this has caused you.