Community Memorial Health System
Where Excellence Begins with Caring
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

F4984-L01-0000001 P001 T00001 **********MIXED AADC 159
SAMPLE A SAMPLE
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

April 27, 2020

Dear Sample A Sample:

Notice of Data Breach

At Community Memorial Health System ("CMHS"), we value our employees and protecting your personal information is our priority. We are writing to let you know about a data security incident involving your personal information.

What Happened?	We were notified by PaperlessPay Corporation ("PaperlessPay") in a letter dated March 20, 2020, that on February 19, 2020, they were contacted by the Department of Homeland Security ("DHS") regarding a possible breach of their systems. PaperlessPay is a vendor hired by CMHS to house pay stubs and assist with W-2 forms. DHS notified PaperlessPay that there was an unknown person purporting to sell "access" to their client database on the dark web. In response, PaperlessPay shut down their web server and SQL server to prevent potential unauthorized access. During this time, CMHS and its employees experienced an interruption in service for a short amount of time while their servers were offline. Over the following weeks, PaperlessPay cooperated with the joint investigation conducted by DHS and the Federal Bureau of Investigation ("FBI"). In addition, PaperlessPay retained a cybersecurity firm to help with their own internal forensic investigation of the incident. Through these investigations, PaperlessPay confirmed that the unauthorized person gained access to their SQL server, where data is stored, on February 18, 2020. The available evidence has not, however, allowed DHS, the FBI, or the security firm to determine what data the person may have accessed or viewed while connected to the SQL server.
What Information Was Involved?	The impacted server stored pay stub and tax forms that contain name, address, pay and withholdings information, bank account number information (if this appears on your paystub), and Social Security number. With respect to bank account information, note that bank information for employees who receive a single deposit was not provided to Paperless Pay. Bank account information is, however, provided for those employees who receive multiple deposits. Specifically, for multiple deposit employees, PaperlessPay would have had access to a full bank account number for each account that is being deposited, but not to bank account routing numbers or bank names.

What are We Doing?	Following notice of this incident, we have been working with PaperlessPay to understand the full scope of the incident and to ensure that CMHS information is secure moving forward. These conversations will be ongoing, but we are able to report that PaperlessPay has taken several steps to improve the security of their systems. Though we can't be certain if the incident exposed your personal information, we believe in taking every precaution here. Therefore, CMHS has arranged for affected individuals to register for identity theft protection and credit monitoring services for one year at no cost to the employee through Experian's® IdentityWorks℠, as described in more detail below.
What You Can Do.	As a precautionary measure, and as noted in our e-mail to you on April 15, 2020, we have asked PaperlessPay to reset all passwords and we recommend that you change the password/access information for your payroll account. Additionally, and as always, please remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC"). Some detailed steps for you to consider are as follows: ● Enroll in Identity Protection Services: To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below: • Ensure that you **enroll by**: **July 31, 2020** (Your code will not work after this date.) • **Visit** t[redacted] • Provide your **activation code**: [redacted] 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 [redacted] by **July 31, 2020.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian. Further information is enclosed at the end of this letter. ● Review Your Account Statements for Suspicious Activity As a precaution, you should review your account statements for any suspicious activity. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your

	state attorney general, and/or the Federal Trade Commission. To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. ● Monitor Your Credit Reports We also recommend you monitor your credit reports. Under US law, you may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Alternatively, you can contact any of the major credit reporting bureaus to request a copy of your credit report. You may also request that these bureaus place a fraud alert on your file at no charge. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below: Equifax (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374 Experian (888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626 TransUnion (800) 916-8800 www.transunion.com P.O. Box 6790 Fullerton, CA 92834 ● Place a Fraud Alert or Security Freeze on Your Credit Report We recommend placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. ● Review Additional Free Resources on Identity Theft You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).
For More Information	For more information, call [redacted] with questions.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [redacted]. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [redacted]. You will also find self-help tips and information about identity protection at this site.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at [redacted].

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.