Community Memorial Health System
Where Excellence Begins with Caring
Processing Center ● P.O. BOX 141578 ● Austin, TX 78714

00001
ACD1234

00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

September 5, 2017

Dear John Sample:

Notice of Data Breach

You are a valued patient of Community Memorial Health System ("CMHS"), 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

On June 22, 2017, a CMHS employee's CMHS e-mail account was compromised via a phishing e-mail. On June 23, 2017, the employee noticed anomalies in their e-mail account and called CMHS' help desk, which resulted in their account password being reset. This also prompted CMHS to launch an investigation to determine the scope of the incident and identify personal information that could have been accessed or acquired as a result of the incident. On or around July 7, 2017, CMHS discovered that the subject e-mail account contained personal information, prompting CMHS to engage a forensic consultant to determine whether a breach may have occurred.

On July 25, 2017, CMHS' forensic consultant reported to CMHS that the markings of the attack indicate that no personal information was accessed but the consultant could not conclude this with absolute certainty. Even though it is highly unlikely that any personal information was accessed or acquired as a result of the attack, in an abundance of caution, CMHS is providing you with this notice regarding the incident.

What Information Was Involved

Based on what we know so far, the types of personal information in the compromised e-mail account generally included patient names, CMHS Medical Record Numbers and/or CMHS Account Numbers, date(s) of service, and certain health information. The information did not, however, include your social security number, bank account, debit card or credit card information.

What We Are Doing

In response to this incident, CMHS has taken steps to mitigate the incident and the effects of the incident, including temporarily disabling all external access to CMHS' e-mail system, ensuring the affected employee updated their e-mail account with a new complex password, engaging a consultant to conduct forensics on the compromised e-mail account, updating its risk analysis, deploying additional alerts and monitoring tools within its server environment, and providing its workforce members with additional training regarding phishing emails.

Even though your personal information is unlikely to have been accessed or acquired, as an additional precaution, CMHS has arranged to offer affected individuals identity theft protection and credit monitoring services for 24 months at no cost to the patient through AllClear ID, as described in more detail below.

What You Can Do

We recommend the following steps that you can take to protect your information:

- Credit Report Monitoring:

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-742-6164 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-742-6164 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

- 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	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	535 Anton Blvd., Suite 100	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	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.

- 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).

<u>More Information</u>

For further information and assistance, please contact our call center at this toll free number 1-855-742-6164.

Sincerely,

Emilie Rayman, Esq.
General Counsel
Community Memorial Health System

Community Memorial Health System
Where Excellence Begins with Caring
Processing Center ● P.O. BOX 141578 ● Austin, TX 78714

00820
00002
ACD1234
TO THE PARENT OR GUARDIAN OF
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

September 5, 2017

Dear Parent or Guardian of John Sample:

Notice of Data Breach

Your above-named child is a valued patient of Community Memorial Health System ("CMHS"), and protecting your child's personal information is our priority. We are writing to let you know about a data security incident involving your child's personal information.

What Happened

On June 22, 2017, a CMHS employee's CMHS e-mail account was compromised via a phishing e-mail. On June 23, 2017, the employee noticed anomalies in their e-mail account and called CMHS' help desk, which resulted in their account password being reset. This also prompted CMHS to launch an investigation to determine the scope of the incident and identify personal information that could have been accessed or acquired as a result of the incident. On or around July 7, 2017, CMHS discovered that the subject e-mail account contained personal information, prompting CMHS to engage a forensic consultant to determine whether a breach may have occurred.

On July 25, 2017, CMHS' forensic consultant reported to CMHS that the markings of the attack indicate that no personal information was accessed but the consultant could not conclude this with absolute certainty. Even though it is highly unlikely that any personal information was accessed or acquired as a result of the attack, in an abundance of caution, CMHS is providing you with this notice regarding the incident.

What Information Was Involved

Based on what we know so far, the types of personal information in the compromised e-mail account generally included patient names, CMHS Medical Record Numbers and/or CMHS Account Numbers, date(s) of service, and certain health information. The information did not, however, include your child's social security number, bank account, debit card or credit card information.

What We Are Doing

In response to this incident, CMHS has taken steps to mitigate the incident and the effects of the incident, including temporarily disabling all external access to CMHS' e-mail system, ensuring the affected employee updated their e-mail account with a new complex password, engaging a consultant to conduct forensics on the compromised e-mail account, updating its risk analysis, deploying additional alerts and monitoring tools within its server environment, and providing its workforce members with additional training regarding phishing emails.

Even though your child's personal information is unlikely to have been accessed or acquired, as an additional precaution, CMHS has arranged to offer affected individuals identity theft protection and credit monitoring services for 24 months at no cost to the patient through AllClear ID, as described in more detail below.

What You Can Do

We recommend the following steps that you can take to protect your child's information:

- Credit Report Monitoring:

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-742-6164 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. To use this service, you will need to provide your child's personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-742-6164 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

- Review Your Child's Account Statements for Suspicious Activity

As a precaution, you should review your child's 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 child's credit reports. Typically, credit is not granted to individuals under the age of 18, and therefore the credit reporting agencies may not maintain a credit file on your child. Children may, however, have a credit report if they are listed as authorized users or joint account holders on an adult's account, or any time a credit account is reported by a lender for that individual. Or your child may have a report if he or she is a victim of identity theft. Under US law, you may obtain a free copy of your child's 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 child's credit report. You may also request that these bureaus place a fraud alert on your child's file at no charge. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your child's credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	535 Anton Blvd., Suite 100	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	Fullerton, CA 92834

- Place a Fraud Alert or Security Freeze on Your Child's Credit Report

We recommend placing a fraud alert on your child's credit report. An initial fraud alert is free and will stay on your child's credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your child's report and requests that the creditor contact you prior to establishing any accounts in your child's name. To place a fraud alert on your child's credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

- 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).

<u>More Information</u>

For further information and assistance, please contact our call center at this toll free number 1-855-742-6164.

Sincerely,

Emilie Rayman, Esq.
General Counsel
Community Memorial Health System

02-02-2

Community Memorial Health System
Where Excellence Begins with Caring
Processing Center ● P.O. BOX 141578 ● Austin, TX 78714

00003
ACD1234

00957
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

September 5, 2017

Dear John Sample:

Notice of Data Breach

You are a valued patient of Community Memorial Health System ("CMHS"), 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

On June 22, 2017, a CMHS employee's CMHS e-mail account was compromised via a phishing e-mail. On June 23, 2017, the employee noticed anomalies in their e-mail account and called CMHS' help desk, which resulted in their account password being reset. This also prompted CMHS to launch an investigation to determine the scope of the incident and identify personal information that could have been accessed or acquired as a result of the incident. On or around July 7, 2017, CMHS discovered that the subject e-mail account contained personal information, prompting CMHS to engage a forensic consultant to determine whether a breach may have occurred.

On July 25, 2017, CMHS' forensic consultant reported to CMHS that the markings of the attack indicate that no personal information was accessed but the consultant could not conclude this with absolute certainty. Even though it is highly unlikely that any personal information was accessed or acquired as a result of the attack, in an abundance of caution, CMHS is providing you with this notice regarding the incident.

What Information Was Involved

Based on what we know so far, the types of personal information in the compromised e-mail account generally included patient names, CMHS Medical Record Numbers and/or CMHS Account Numbers, date(s) of service, and certain health information. In your case, in addition to the various types of information listed above, the information also may have included your social security number. The information did not, however, include your bank account, debit card or credit card information.

What We Are Doing

In response to this incident, CMHS has taken steps to mitigate the incident and the effects of the incident, including temporarily disabling all external access to CMHS' e-mail system, ensuring the affected employee updated their e-mail account with a new complex password, engaging a consultant to conduct forensics on the compromised e-mail account, updating its risk analysis, deploying additional alerts and monitoring tools within its server environment, and providing its workforce members with additional training regarding phishing emails.

Even though your personal information is unlikely to have been accessed or acquired, as an additional precaution, CMHS has arranged to offer affected individuals identity theft protection and credit monitoring services for 24 months at no cost to the patient through AllClear ID, as described in more detail below.

What You Can Do

We recommend the following steps that you can take to protect your information:

- Credit Report Monitoring:

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-742-6164 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-742-6164 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

- 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	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	535 Anton Blvd., Suite 100	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	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.

- 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).

<u>More Information</u>

For further information and assistance, please contact our call center at this toll free number 1-855-742-6164.

Sincerely,

Emilie Rayman, Esq.
General Counsel
Community Memorial Health System