UMC
UNIVERSITY MEDICAL CENTER

October 4, 2021

Sent Via Certified Mail
The Honorable Attorney General Wayne Stenehjem
Office of the Attorney General of North Dakota
600 East Boulevard Avenue, Department 125
Bismark, ND 58505-0040

Re: University Medical Center of Southern Nevada Cybersecurity Breach

Dear Attorney General Stenehjem:

I write on behalf of University Medical Center of Southern Nevada ("UMC"), a county-owned hospital located in Las Vegas, Nevada. On June 14, 2021, UMC experienced a cyberattack in which certain files on the hospital's network servers were compromised. UMC's Information Technology Department acted swiftly to secure the hospital's network and end the compromise on June 15, 2021.

To the best of our knowledge, no clinical systems were accessed by the criminals. However, the files that were compromised contained personally identifiable information (PII), including protected health information (PHI). Information about affected individuals, such as demographic information (e.g., name, address, date of birth, Social Security Number), clinical information (e.g., diagnosis, test results), or financial information (e.g., insurance number) may have been included in the files compromised by the cybercriminals responsible for the attack.

As you are aware, cyberattacks such as the one UMC experienced are increasingly common among hospitals and other organizations across the world. The criminals who engaged in the cyberattack against UMC did so for monetary gain. Even though UMC is not located in your state, the cyberattack affected residents of your state who at some point received treatment from UMC. UMC notified approximately 292 individuals in your state via certified mail. Enclosed with the notification was an offer by UMC to provide complementary identify protection services for those individuals affected by the cyberattack. *See* Enclosures.

UMC is providing this notification to your office in order to make you aware of our ongoing efforts to assist the residents of your state. We also hope that it will satisfy any requirements you have from a state reporting prospective. On August 13, 2021, UMC reported the cyberattack to the Office of Civil Rights at the United States Department of Health and Human Services, and the incident was assigned the Breach Tracking Number of VT544J8SM2. UMC has been in communication with various law enforcement agencies, including the Federal Bureau of Investigation, the Las Vegas Metropolitan Police Department and the Nevada Attorney General's Office.

Should you have any additional questions, please contact me via telephone at (702) 383-3854 or via email at keith.slade@umcsn.com

Sincerely,

/s/ Keith Slade

Keith Slade
Privacy Officer

RECEIVED
OCT 08 2021
OFFICE OF ATTORNEY GENERAL
FINANCE DIVISION

Encl.: As noted.

P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
(833) 909-3920
Or Visit:
https://response.idx.us/umcsn
Enrollment Code: <<Enrollment Code>>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

PERSONAL AND CONFIDENTIAL

August 2, 2021

Re: Notification of Data Security Incident

Dear << Parent or Guardian of >> <<FirstName>> <<LastName>>:

We are sending this letter to you as part of University Medical Center of Southern Nevada's (UMC) commitment to privacy. UMC takes its responsibility to protect your information and your privacy very seriously. We are informing you of a data security incident involving UMC.

UMC's cyber security team recognized suspicious activity on the hospital's computer network in mid-June and responded by immediately restricting external access to UMC servers. Based on what we have discovered so far, the compromise began on June 14, 2021, and UMC was able to end the compromise on June 15, 2021.

Unfortunately, cyberattacks have become increasingly common in the health care industry, with hospitals across the world experiencing similar situations. Affected information, potentially including yours, was compromised by a well-known group of cybercriminals that seek to use the information for commercial gain.

We have no evidence to date that UMC's clinical systems, including those interfaced with our electronic health record, were accessed. However, we have determined that certain files on our network servers were compromised. Among other information, these files contain personally identifiable information (PII), to include certain protected health information (PHI), used for reporting, tracking and other purposes needed for the proper operation of UMC. While we have no direct evidence of the misuse of your specific information, UMC is notifying individuals about the incident so you can take steps to protect your identity. Information about you, such as demographic information (name, address, date of birth, Social Security Number), clinical information (history, diagnosis, test results) or financial information (insurance number) may have been included in the information compromised by these cybercriminals.

UMC has notified the FBI and the Las Vegas Metropolitan Police Department. In addition, UMC is currently engaged in a number of security initiatives, including working closely with external cyber security professionals, and updating internal and external technology solutions in order to further strengthen UMC from cyberattacks.

UMC has also partnered with IDX, an identity protection company, to offer you complimentary identity protection services. Your enrollment code is included with this letter, and can be used to enroll at: https://response.idx.us/umcsn. If you are unable to enroll on-line, a toll free number is available at: (833) 909-3920. Both the enrollment website and the toll-free number are also available to provide additional information and answer any questions you may have. We encourage you to take the opportunity to learn more about this incident and consider enrolling in the identity protection services we are offering. Your opportunity to enroll will expire 90 days from the date of this letter.

Product Description: You are receiving an individual code allowing you to enroll in 12 months of Single Bureau Credit Monitoring services. CyberScan also monitors criminal websites, chat rooms, and bulletin boards for illegal selling or trading of their personal information. In addition, IDX will keep you up-to-date on new identity theft scams, tips for protection, legislative updates, and other topics associated with maintaining the health of your identity. You will also have access to the IDX team and the online resource center for news, education, and complete recovery services. In the event of a confirmed identity theft, you may be eligible for reimbursement of up to $1,000,000 for expenses related to that theft. You will receive full ID theft restoration services should you fall victim

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://response.idx.us/umcsn and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. **Activate the CyberScan monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. **Telephone.** Contact IDX at (833) 909-3920 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. **Watch for Suspicious Activity**. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. **Security Freeze.** You may place a free credit freeze for children under age 16. By placing a security freeze, someone who fraudulently acquires your child's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your child's credit files.

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

6. **You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.