MEDICINE LODGE MEMORIAL HOSPITAL & PHYSICIANS CLINIC

May 17, 2021

MLMH&PC received notification from its business associate, CaptureRx, a 340B third party administrator about a security incident involving the breach of unsecured protected health information (PHI) for MLMH&PC's patients. As a result of the incident, CaptureRx notified Medicine Lodge Memorial Hospitals Facility patients of a breach of unsecured PHI after discovering the following event:

Brief Description of What Happened and Description of the Types of Unsecured PHI

CaptureRx became aware of unusual activity involving certain files on its network. These files contained PHI related to services that its provides to healthcare providers. Following discovery of the unusual activity, CaptureRx commenced an investigation into this activity and the overall security of its network. On February 19, 2021, CaptureRx determined that certain files were accessed without authorization on February 6, 2021. CaptureRx immediately began a comprehensive review of the specific files accessed to determine whether PHI was contained within those files at the time of the incident. CaptureRx completed its review on or around March 19, 2021, confirming that PHI related to MLMH&PC patients was contained within the files accessed on February 6, 2021.

On or about April 6, 2021, CaptureRx provided MLMH&PC with notice of the incident and preliminary information related to CaptureRx's investigation. Since that time, MLMH&PC has been in contact with CaptureRx in order to determine the MLMH&PC patients that may have been impacted; the types of PHI involved; information related to CaptureRx's investigation; the manner of access; whether the data was exfiltrated from CaptureRx's system; and CaptureRx's mitigation efforts. The unsecured information includes: patient first and last name; date of birth; prescription number; fill date; date written; National Drug Code (unique, 3-digit numeric identifier attached to each medication listed under Section 510 of the U.S. Federal Food, Drug and Cosmetic Act); drug description; prescriber name and National Provider Identifier (unique, 10-digit numeric identifier to identify healthcare providers); and BIN/PCN/GID (unique numbers that identify the patient and his/her Medicare Part D prescription drug plan).

Investigation, Mitigation, and Protection Against Future Breaches

CaptureRx immediately commenced an investigation into this breach. CaptureRx retained Charles River Associates (CRA) to perform a third-party forensic investigation. CRA identified a vulnerability that allowed access to a build server, which was exploited by a Threat Actor. This resulted in the Threat Actor gaining credentials into one S3 bucket, which were

leveraged to extort CaptureRx. CRA performed a complete forensic analysis and determined that the Threat Actor's access was limited to one S3 bucket housed on a third-party build server. There was no authorized access to CaptureRx's network itself. CRA advised CaptureRx that the identified vulnerability was fully remediated as part of CRA's forensic review.

CRA also determined that the impacted data was exfiltrated (the unauthorized transfer of data from an information system) by the Threat Actor. Approximately 1,818 records were exfiltrated. CaptureRx advised MLMH&PC that the Threat Actor subsequently returned the data to CaptureRx. CaptureRx determined that there was no evidence that the exfiltrated data was released or posted in any public manner or on the dark web. The Threat Actor also represented to CaptureRx that it did not misuse the data and no longer has any data in its possession.

Based on the investigation, CaptureRx confirmed the security of its systems; updated all CaptureRx user passwords; hardened firewall rules; implemented workforce training; and is in the process of reviewing and updating information security policies, as appropriate. MLMH&PC has also taken steps and used this incident as an opportunity to review its relationships with business associates; the requirements it sets forth in MLMH&PC business associate agreements with vendors; and maintained communication and asked questions of CaptureRx to learn as much information as possible related to the incident, including what CaptureRx has done to fix the problem.

Steps to Take to Protect Against Potential Harm

While CaptureRx is not aware of any actual or attempted misuse of MLMH&PC patient information, because there is always a concern of identity theft or fraud when personal information is exfiltrated by a Threat Actor, CaptureRx has advised the impacted patients to monitor activity on their credit and other accounts. MLMH&PC advises impacted patients to take the following actions:

1. Call the toll-free numbers of one of the three major credit bureaus to place a fraud alert on their credit reports. This can help prevent identity theft by preventing new accounts from being opened. Ask for copies of credit reports. The three major credit bureaus are:

    a. Equifax 1-800-525-6285 (P.O. Box 740241, Atlanta GA 30374-0241)
    b. Experian 1-888-397-3742 (P.O. Box 9532, Allen, TX 75013)
    c. TransUnion 1-800-680-7289 (Attn: Fraud Victims Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790)

2. Monitor their credit reports. Examine their reports closely for activity that the Patient has not initiated.

3. Monitor banking and credit card statements closely for activity that the Patient has not initiated.

4. Visit the Federal Trade Commission Identity Theft website for information on

identity theft protections. www.ftc.gov (to Quick Finder and click on Identity Theft).

5. Refer to the "Steps You Can Take to Protect Personal Information" provided CaptureRx in its notification letter. Patients can also contact CaptureRx at the toll free number provided in the notification letter.

MLMH&PC takes seriously its role in maintaining the privacy and security of patient information. If a patient has questions or wants additional information, he/she can direct those to CaptureRx at the contact information provided in the CaptureRx notification letter. Patients can also call the Facility and speak to our Privacy Officer, at Medicine Lodge Memorial Hospital. The Privacy Officer may also be reached at jdavis@mlmh.net or 710 N Walnut Medicine Lodge, KS 67104. Patients are also welcome to come to MLMH&PC and speak with us in person. We apologize for any inconvenience, stress, or worry that this event may cause you.

Sincerely,

Ashley Taylor
Chief Executive Officer