

Cherokee Regional Medical Center was recently notified of a data breach by a company that provided mobile imaging services to some of our patients. Below is a copy of the notice. The notice is also available at <https://www.dmshealth.com/notice-of-data-event/>.



## **DMS HEALTH TECHNOLOGIES PROVIDES NOTICE OF DATA EVENT**

DMS Health Technologies (“DMS”) recently discovered a data security event that may impact the confidentiality and security of information related to certain patients as well as current or former employees of DMS. As we continue to work toward notifying impacted patients directly, we are providing information about the event, our response, and steps potentially impacted individuals can take to better protect against the possibility of identity theft and fraud, should they feel it is appropriate to do so.

**What Happened?** On April 23, 2023, DMS became aware of suspicious activity related to certain computer systems. We immediately launched an investigation, with the assistance of third-party forensic specialists, to secure our network and determine the nature and scope of the activity. The investigation determined that there was unauthorized access to DMS’s network between March 27 and April 24, 2023, and the unauthorized actor had the ability to access certain information stored on the network during the period of access. Therefore, we undertook a comprehensive review of the files determined to be at risk to identify whose information may have been impacted by this event. Once this comprehensive review is complete, we will continue to work as quickly as possible to mail notification letters directly to potentially impacted individuals, which will include resources that individuals can reference to further protect their information.

**Which Patients / What Information was Affected?** The type of information potentially may vary by individual but typically is limited to name, date of birth, date of service, physician name, and exam type.


**What We Are Doing?** We take this event and the security of your information very seriously. Upon learning of this event, we immediately took steps to secure our network and maintain operations in a safe and secure manner. As part of our ongoing commitment to the privacy of personal information in our care, we are reviewing our existing policies and procedures and plan to implement additional administrative and technical safeguards to further secure our systems. Notice was also provided to federal law enforcement and to the U.S. Department of Health and Human Services.

**What Affected Individuals Can Do.** Potentially affected individuals are encouraged to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits. You can also find out more about how to safeguard your information by reviewing the below Steps You Can Take to Help Protect Personal Information.

**For More Information.** If you have questions, you may call our dedicated assistance line at: (866) 373-7164 Monday through Friday from 8:00 am to 10:00 pm CT or Saturday and Sunday from 10:00 am to 7:00 pm CT (excluding major U.S. holidays). You may also write to DMS directly at 728 East Beaton Drive, Suite 101, West Fargo, ND 58078.

## **STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION**

**Monitor your credit reports for suspicious or unauthorized activity.** Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

 **Place a fraud alert on your credit file.** Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take

steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

**Place a security freeze on your credit file.** As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

**EQUIFAX**

[https://www.equifax.com/personal/credit-report-services/  
1-888-298-0045](https://www.equifax.com/personal/credit-report-services/1-888-298-0045)

Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069  
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788

## **EXPERIAN**

<https://www.experian.com/help/>

1-888-397-3742

Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013

Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013

## **TRANSUNION**

<https://www.transunion.com/credit-help>

1-800-916-8800

TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016

TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

## **ADDITIONAL INFORMATION**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.