

Confidentiality Breach Notice

November 15, 2016

This document directly relates to a potential breach of personal health information. In our commitment to our patients and their privacy, it is important to us that all potentially affected individuals are fully informed of the possible breach and are made aware of the steps that should be taken to protect those potentially involved from potential harm as a result of any breach of personal health information.

On or about September 16, 2016, we became aware of a possible breach of patient information when we were notified that a former employee potentially retained a copy of patient personal health information that had been permissibly acquired while employed at our practice. Upon learning of the potential breach of information by the former employee, we took prompt action to investigate this potential privacy issue. We discovered that although we terminated the former employee’s access to our electronic health record system after receiving his resignation on September 9, 2016, we believe that the former employee may have impermissibly retained documents that held the protected health information of patients that the former employee worked with in his role. We believe that the information retained by the former employee may have contained name, address, Social Security number, date of birth, and/or diagnosis. To date, no fraudulent use of any personal health information has been found. While we feel that the number of clients effected is very small, we have notified any and all clients that this employee worked with during his time at CMHS. The number of people that may have potentially been effected is 132.

Even though we have not received any reports about the further use or disclosure of any personal health information by the former employee, there may still be risk for identity theft. We advise anyone who may have been effected to immediately take the following steps:

* **Place a fraud alert on your credit file.** Call the toll-free numbers of any of the three major credit bureaus (identified below) to place a fraud alert on your credit report. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three bureaus will provide you a copy of your credit report free of charge.

**Equifax:** (888)766-0008; [www.fraudalerts.equifax.com](http://www.fraudalerts.equifax.com). General: (800) 685-1111, [www.equifax.com](http://www.equifax.com), P.O. Box 740241, Atlanta, GA 30374-0241.

**Experian: (888) 397-3742:** <https://www.experian.com/fraud/center.html>. General: (888)EXPERIAN (397-3742); [www.experian.com;](http://www.experian.com) 475 Anton Blvd., Costa Mesa, CA 92626.

**TransUnion:** (800) 680-7289 (888-909-8872 for freeze); <http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page>; TransUnion Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA 19022-2000. General: (800) 680-7289; [www.transunion.com](http://www.transunion.com); P.O. Box 2000, Chester, PA 19022-2000

* **Closely examine your credit report upon receipt.** Carefully review your credit report for signs of fraud, such as credit accounts that are not yours, accounts that you do not remember opening, and/or requests from creditors that you do not know about. Make sure all the information in your report is correct. Check to ensure that there are not any medical bills that you do not know about. Call the credit agency if you have any questions about the information in your credit report.
* **Immediately contact your local police or sheriff’s office if there is something wrong with your report.** File an identity theft report if your credit report indicates that fraudulent activity may have occurred. Request and retain a copy of your filed theft report. You may need to give a copy of the theft report to creditors. The state of Missouri provides a sample letter for your use to dispute any fraudulent charges, which is available at: <https://ago.mo.gov/docs/default-source/publications/dispute-letter-for-exisiting-accounts.doc?sfvrsn=2>.
* **Continue to monitor your credit reports.** Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure that an imposter has not opened an account with your personal information. Check your credit report every three months for the next year.
* **Review additional online resources about identity theft.** The federal government offers a one-stop resource for identity theft matters, which is available at: <https://www.identitytheft.gov>.

You may also want to review the state of Missouri’s online Identity Theft Resource Guide at: <https://ago.mo.gov/docs/default-source/publications/identitytheft.pdf?sfvrsn=2>.

* **Keep a copy of this letter for your records**. This correspondence can help if you have future problems with your medical records. You may want to ask for a copy of your medical records from your healthcare providers. It is good to have a copy that you can look at in case you ever have problems.

Our investigation into this potential breach incident remains open. To protect against such breaches in the future, we have hired an outside entity to assist us in our investigation. The results of this investigation will be used to determine whether the imposition of any workforce sanctions is warranted, to develop more extensive staff training on the privacy and security of patient information, and to implement any necessary revisions to our policies and/or procedures regarding patient privacy. We have also requested the former employee to return all patient information that may have been impermissibly retained. We will dispose of this information in a proper manner once it has been returned.

We regret the occurrence of this potential breach incident and sincerely apologize for any inconveniences that this situation may cause. Please be assured that we are fully committed to keeping our client’s information safe.

Any questions about this incident or if there is additional information needed on what should be done as a result of the breach, please contact our Privacy Officer Gina Armitage, Director of Quality and Compliance at one of the following options:

816-836-6788

GArtmitage@thecmhs.com

PO Box 260

Independence, Mo 64051

Hours of operation: Monday – Friday 8:00 – 4:30

Sincerely,

Julie Pratt

Vice President of Operations