Re: Important Notice Regarding Possible Disclosure of Private Information

This notice is to inform impacted individuals about a recent IT incident at Central Minnesota Mental Health Center ("Company") that may affect the security of your personal information and/or personal health information. At present, we have no evidence that any of the personal information or personal health information on Company's system was used maliciously; however, in an abundance of caution, we want to notify you of the IT incident and offer you the resources discussed below. We take this incident seriously, and as such, are providing you with information and access to resources so that should you feel it is appropriate to do so, you can protect your personal information.

What Happened? On October 21, 2021, Company became aware of potentially malicious activity on the Company's email accounts. Upon discovery, Company immediately secured their email accounts and launched an investigation with the help of third-party IT forensic investigators to determine the scope and extent of unauthorized access and whether any sensitive information was exfiltrated. On or around November 23, 2021, the third-party forensic investigator confirmed that multiple email accounts had been synced, and thus were considered compromised. The investigation revealed that the IT incident began on September 20, 2021 and continued until the environment was secured by the Company on October 29, 2021. After receiving confirmation of the compromised accounts, the Company immediate engaged a third-party specialist to review the effected accounts and create a list of individuals whose personal information or personal health information was impacted. On February 14, 2022, it was determined that the compromised email accounts contained personal information or personal health information about certain individuals, including your information.

What Information Was Involved? The data that was contained in the impacted email accounts was different in individual cases; however, in that vast majority of cases, the data at issues was medical data including clinical information, mailing addresses, patient account number, treatment location, doctor's name and treatment/procedure information. In less common situations, the emails contained names, telephone numbers, date of birth, Social Security number, and, in some instances, driver's license number, and/or credit card/financial account numbers.

What Are We Doing? We take the security of sensitive information very seriously. Upon discovery of this incident, company immediately secured our systems and took steps to prevent further unauthorized access. The problem has been remediated and our IT systems are operating securely. In addition to conducting a thorough investigation into the incident with the help of a qualified third-party IT forensic investigator, we implemented additional safeguards and security measures to enhance the privacy and security of information in our systems.

We also want to make sure you have the information you need so that you can take steps to help protect yourself and your identity. We encourage you to remain vigilant and to regularly review and monitor relevant account statements and credit reports and report suspected incidents of identity theft to local law enforcement, your state's Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps in this letter.

Complimentary Identity Protection and Credit Monitoring Services

Because of the potential release of private information, we are offering at no charge to impacted individuals, identity theft protection services through Equifax. Equifax's service, called Equifax Credit Watch™ Gold, includes: Twelve [12] months credit file monitoring, unlimited access to your Equifax credit report and credit score, WebScan notifications when your personal information is found on fraudulent Internet trading sites, fraud alerts, a $1,000,000 insurance policy, and additional identity restoration programs. With this protection, Equifax Credit Watch™ Gold will help you resolve issues if your identity is compromised.

On behalf of Company, we are genuinely sorry this incident occurred and apologize for any inconvenience this matter may cause you. We can assure you that we are doing everything we can to protect you and your information, now and in the future. If you have questions about this notice or this incident, or believe your information was impacted, you can reach us at 855-604-1867 between the hours of 8:00 a.m. and 8:00 p.m. (CST).