16920

[PRINT ON COMPANY LETTERHEAD]

May 11, 2020

[Name]
[Address 1]
[Address 2]
[City, State Zip Code]

NOTICE OF DATA BREACH

Dear [Name]:

We are writing to inform you of a security incident involving certain personal information maintained by Mille Lacs Health System ("MLHS"). We are providing this notice as a precaution to inform potentially affected individuals about the incident and to call your attention to some steps you can take to help protect yourself. We sincerely regret any concern this may cause you.

What Happened?
On November 14, 2019, we learned that an outside entity sent phishing emails to certain of our employees soliciting their login information to our email system. We immediately commenced an investigation and determined on February 24, 2020, that the entity appears to have been able to use employee credentials to gain unauthorized access from August 26, 2019 through January 7, 2020 to a small number of employee email accounts. On April 22, 2020, our data review experts determined that protected health information belonging to some of our patients was contained within the impacted accounts and therefore was potentially accessed. We have terminated the unauthorized access to our employee email accounts. The access was limited to information that was contained in emails of the impacted employees and did not extend to patient databases.

What Information Was Involved?
The information stored in the affected email accounts varies by individual, but may include first and last name, addresses, date of birth, provider name, date of service, clinical information, treatment information, procedure type and in some cases social security numbers. Based on our investigation, it appears you were one of the individuals whose information was contained in the emails that were accessed, and therefore your information could be affected by this incident. Our investigation has not found any evidence that this incident involves any unauthorized access to or use of any of MLHS's other internal computer systems or network. We are not aware of any fraud or misuse of your information as a result of this incident.

What We are Doing.
We take the privacy of personal information seriously and deeply regret that this incident occurred. We took steps to address this incident promptly after it was discovered, including initiating an investigation into this incident and working with an independent forensic investigation firm to assist us in the investigation of and response to this incident. Additionally, we have reset all user account passwords and have implemented additional technology measures in order to help prevent this type of incident from reoccurring in the future.

While there is no evidence of any misuse of your information, out of an abundance of caution, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 18 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do.
We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-833-979-2230 or going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 8:00 am – 8:00 pm Central Time. Please note the deadline to enroll is [Enrollment Deadline].

You can also review the enclosed supplemental information. In addition, we advise you to report suspected incidents of identity theft to local law enforcement or the Attorney General.

For More Information.
For more information about this incident, or if you have additional questions or concerns, please call 1-833-979-2230 between the hours of 8:00 am and 8:00 pm Central Time, Monday through Friday or go to https://app.myidcare.com/account-creation/protect. Again, we sincerely regret any concern this incident may cause.

Sincerely,

Bill Nelson
Chief Executive Officer

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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

3. **Telephone.** Contact MyIDCare at [TFN] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. **Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare 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. **Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above 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 credit files.

7. 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.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.