Attachment 1

MICHIGAN MEDICINE
UNIVERSITY OF MICHIGAN

Corporate Compliance Office
Return Mail to IDX
P.O. Box 1907
Suwanee, GA 30024

<<Variable 1>>
<<First Name>> <<Middle Name or Initial>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip>>

October 26, 2022

RE: Patient – <<First Name>> <<Middle Name or Initial>> <<Last Name>>

Dear <<Variable 1>> <<First Name>> <<Middle Name or Initial>> <<Last Name>>,

We are writing to let you know about an incident that may have exposed the above-named patient's personal and health information and to explain what happened. **Please note that your Social Security Number, credit card, debit card or bank account numbers were *not* involved in this incident.** Patient privacy is important to us, and we take this matter very seriously.

What Happened & Information Involved

From August 15 through August 23, 2022, a cyber attacker targeted Michigan Medicine employees with an email "phishing" scam. In this scam, the attacker lured employees to a webpage designed to get them to enter their Michigan Medicine login information. A few Michigan Medicine employees entered their login information and then inappropriately accepted multifactor authentication prompts which allowed the cyber attacker to access their Michigan Medicine e-mail accounts. Michigan Medicine learned the email accounts were compromised on August 23, 2022, the accounts were immediately disabled so no further access could take place and password changes were made.

No evidence was uncovered during our investigation to suggest that the aim of the attack was to obtain patient health information from the compromised email accounts, but data theft could not be ruled out. As a result, the email accounts and their contents were presumed compromised. Thus, all the emails and any attachments to them required a detailed, thorough review to determine if sensitive data about one or more patients was potentially impacted. This review was completed on October 17, 2022. Immediately thereafter, Michigan Medicine engaged a vendor to assist in the mailing of patient notice letters.

Some emails and attachments were found to contain identifiable patient information such as: Name; medical record number; address; date of birth; diagnostic and treatment information; and/or health insurance information. The emails were job-related communications for coordination and care of patients, and information related to a specific patient varied, depending on a particular email or attachment. Your Social Security Number, credit card, debit card or bank account numbers were not involved in this incident.

Steps We are Taking in Response

We regularly provide training and education materials to increase employee awareness of the risks of cyberattacks. This includes sending regular, simulated phishing emails (imitations) that we initiate and manage so employees are trained on what to look for, and how to identify and report them. The employees involved in this incident had previously been involved in these training exercises. This incident happened because they failed to follow our policies, particularly by accepting unsolicited multifactor authentication prompts. They are subject to disciplinary action under Michigan Medicine policies and procedures. We are also assessing the ability to place additional technical safeguards on our email system and the infrastructure that supports it to prevent similar incidents from happening.

Steps to Protect Yourself

We believe the risk of identity or medical theft is low because your Social Security Number, credit card, debit card or bank account numbers were not involved**.** If you have any questions, please call the toll-free Michigan Medicine Assistance Line: 1-833-814-1736. Calls will be answered by the Michigan Medicine Assistance Line between 9 am to 9 pm (Eastern Time), Monday through Friday, except holidays.

Additionally, we always recommend that patients monitor insurance statements for any transactions related to care or services that have not actually been received. Information about potential identity theft is available from the Federal Trade Commission at www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft. We have also enclosed a list of recommendations for all persons to take to prevent and detect potential identity theft.

We are very sorry and deeply regret this incident has happened. We are taking the proper steps to reduce the chance of this happening again. Michigan Medicine reported this incident to law enforcement. We are also notifying the U.S. Department of Health and Human Services Office for Civil Rights about this incident. If you have any questions or concerns, please call us at the number above. We apologize for any stress this situation may cause and assure you that we are committed to doing everything possible to protect your information and regain your trust.

Sincerely,

Jeanne M. Strickland
Chief Compliance Officer
Michigan Medicine Corporate Compliance Office

Enclosure

ATTACHMENT

You can take the following steps to monitor for your account and credit report activity:

- Contact your health insurance company to review any claims that may not pertain to prescription and/or health care services that you actually received;
- Contact your pharmacy to review any activity that may not pertain to prescriptions that you actually received.
- Contact your healthcare provider if bills you expect to receive do not arrive on time
- Review all credit card information;
- Review other financial account information;
- Watch your accounts for activity that may not be yours; and
- Contact the place where you have the account immediately if you notice anything might be wrong

Your Credit Report: In addition to the above, if you have concerns, you may review your credit report. Credit reports contain information about you, including what accounts you have and your bill paying history.

- The law requires the major nationwide credit reporting companies – Equifax, Experian and TransUnion - to give you a free copy of your credit report every 12 months if you ask for it.
  - Visit https://www.annualcreditreport.com/index.action or call 1-877-322-8228, a service created by these three companies to order your free annual credit report. You also can write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.
  - If you see accounts or addresses you don't recognize or information that is inaccurate, contact the credit reporting company and the information provider. To find out how to correct errors on your credit report, visit http://www.consumer.ftc.gov/features/feature-0014-identity-theft

Credit Freeze: If you are concerned about identity theft, you might consider placing a credit freeze on your report. For more information about credit freezes, see:

http://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs