



Corporate Compliance Office
Return Mail to IDX
PO Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

RE: Patient – <<First Name>> <<Middle Name>> <<Last Name>>
Dear <<First Name>> <<Last Name>>,

We are writing to let you know about an incident that may have exposed your 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. We are also not aware that any of your information was misused.** Privacy is important to us, and we take this matter very seriously.

What Happened

From May 23 through May 29, 2024, three (3) Michigan Medicine employee email accounts were compromised due to a cyberattack. The attacker called the Michigan Medicine IT Service Desk and impersonated Michigan Medicine employees to trigger a password reset to obtain the employee's login credentials. Michigan Medicine learned two (2) email accounts were compromised on May 23, 2024, and the third account was compromised on May 29, 2024. As soon as Michigan Medicine learned that the email accounts were compromised, the attacker's IP address was blocked, and immediate password changes were made so no further access could take place.

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 June 27, 2024. Immediately thereafter, Michigan Medicine engaged a vendor to assist in the mailing of patient notice letters.

Information Involved

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 payment and billing coordination for Michigan Medicine patients. The information involved for each specific patient varied, depending on the particular email or attachment. Your Social Security Number,

credit card, debit card or bank account numbers were *not* involved in this incident.

Our Response

Michigan Medicine is taking swift action to ward off future social engineering attacks that target employees. Michigan Medicine has strengthened existing processes for verifying caller identity and resetting passwords through our internal service desk. All Michigan Medicine staff will also receive additional education on how social engineering attacks work, the need to select strong passwords, and the need to use different passwords for multiple sites.

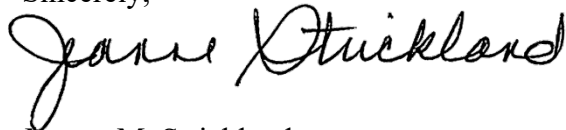
What You Can Do

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. We have partnered with IDX, A ZeroFox Company, to answer questions and provide valuable information about the incident. We encourage you to contact IDX with any questions by calling 1-888-409-7484. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

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
File No. 18305



Recommended Steps to help Protect your Information

- 1. Telephone.** Contact IDX at 1-888-409-7484 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 2. 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.
- 3. Report suspicious activity.** 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.
- 4. 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
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
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.

5. 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.

6. 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. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

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