Central Florida Inpatient Medicine
Provides Notice of Data Security Incident

Central Florida Inpatient Medicine ("CFIM") is committed to maintaining the privacy and security of the information that it maintains. CFIM recently notified individuals of a data security incident involving access to a CFIM employee email account by an unauthorized party.

Upon learning of this issue, CFIM secured the account and commenced a prompt and thorough investigation. As part of its investigation, CFIM engaged external cybersecurity professionals experienced in handling these types of incidents. The investigation worked to identify what personal information, if any, might have been contained in the affected email account. After an extensive forensic investigation and comprehensive and time-consuming manual document review, CFIM discovered on May 5, 2022 that the email account accessed between August 21, 2021 and September 17, 2021 contained identifiable personal and/or protected health information. CFIM has no evidence to suggest that any information has been misused. However, out of an abundance of caution, CFIM provided written notification to anyone whose information may have been contained in the accessed account.

The accessed email account contained the personal and protected health information of certain individuals, including their names, dates of birth, medical information including diagnosis and/or clinical treatment information, physician and/or hospital name, dates of service, and health insurance information. In a limited number of cases, Social Security numbers, driver's license numbers, financial account information, and usernames and passwords were also impacted. This incident does not affect all clients of CFIM and not all information was included for all individuals.

CFIM is sending notification letters to each affected individual for whom we have enough information to determine a physical address. Notified individuals have been provided with best practices to protect their information and have been reminded to remain vigilant in reviewing financial account statements on a regular basis for any fraudulent activity. It has also been recommended that affected individuals review the explanation of benefits statements that they receive from their health insurance providers and follow up on any items not recognized. For the limited number of individuals whose Social Security numbers were contained in the impacted account have been offered complimentary credit monitoring. Additional safeguards are provided below under "Other Important Information".

Since the date of this incident, CFIM has taken measures to improve its technical safeguards in order to minimize the risk of a similar incident in the future, including implementing additional technical safeguards on its email system, implementing multifactor authentication, and providing additional training to employees to increase awareness of the risks of malicious emails.

For further questions or additional information regarding this incident, or to determine if you may be impacted, CFIM has set up a dedicated toll-free response line for individuals to ask questions. The response line can be contacted at (855) 503-3415 and is available Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

– OTHER IMPORTANT INFORMATION –

Placing a Fraud Alert on Your Credit File.

You may place an initial one (1) year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion LLC
P.O. Box 6790
Fullerton, CA 92834-6790
https://www.transunion.com/fraud-alerts
(800) 680-7289

Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(800) 349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.