Notice of Data Security Incident

Dermatology Group of Arkansas, PA ("DGA") is committed to maintaining the privacy and security of information. DGA recently notified individuals of a data security incident involving access to three employee email accounts by an unauthorized third-party as the result of a phishing incident.

Upon learning of this issue, DGA immediately commenced a prompt and thorough investigation, working closely with external cybersecurity professionals. After an extensive forensic investigation and manual document review, DGA discovered on May 10, 2021 that the email accounts that were accessed between November 12, 2020 and December 2, 2020 contained identifiable personal and/or protected health information. DGA has no evidence to suggest that any information has been misused. However, out of an abundance of caution, DGA issued notices to anyone whose information was contained in the accessed accounts.

The accessed email accounts contained the personal and protected health information of certain patients, including their name, date of birth, address, diagnostic/treatment information, medical record number, patient account number, date of service, provider name, surgical information, medication information, and health insurance information. A limited number of individuals' Social Security number, driver's license number, passport number, financial account information, credit card account information, and online user account credentials were also contained in the impacted email accounts. This incident does not affect all patients of DGA and not all of these identifiers were included for each notified individual.

DGA sent notification letters to each potentially affected individual for whom it has enough information to determine a physical address. Notified individuals should monitor insurance statements for any transactions related to care or services that have not actually been received. For the individuals whose Social Security numbers were impacted, complimentary credit monitoring was offered.

The security of the personal information of our patients is DGA's top priority. DGA remains fully committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it.

For further questions or additional information regarding this incident, or to determine if you may be impacted, DGA has set up a dedicated toll-free response line for individuals to ask questions. The response line can be contacted at 877-418-8555 and is available Monday through Friday, 8 am to 5 pm EST.

Other Important Information

Placing a Fraud Alert on Your Credit File

You may place an initial 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 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

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 sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

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 monitoring 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 financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

If 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.

Protecting Your Medical Information.

We have no information to date indicating that medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.

- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.