DuPage Medical Group
WE CARE FOR YOU

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

<<VARIABLE HEADER>>

Dear <<Name 1>>:

As CEO of DuPage Medical Group, Ltd. ("DMG"), I am writing to make you aware of an incident that may affect the security of some of your information. Our community has heard of countless security incidents affecting many organizations across a variety of industries in the recent months. Unfortunately, DMG is among this group of organizations affected. The information below outlines details about the incident, our response, and resources available to you.

What Happened? On July 13, 2021, we experienced a security incident that caused a disruption to our network systems. We immediately began working with third-party cyber-forensic specialists to assist in our investigation to determine the full nature and scope of the incident. It was determined that the network outage was caused by unauthorized actors who gained access to the DMG network between July 12, 2021, and July 13, 2021. Through the investigation, it was discovered that certain systems containing information related to patients may have also been impacted by this event. DMG, with the assistance of the forensic specialists, conducted a thorough and time-consuming review of its systems to understand whether any patient information may have been impacted as a result of this event. On August 17, 2021, we determined that certain files stored within our environment that contained your information may have been impacted by this event.

What Information Was Involved? Our investigation to date has revealed the following types of personal information potentially affected by this incident include your name, address, date of birth, diagnosis code, CPT code (Current Procedural Terminology, also known as service codes, is a universal system that identifies medical procedures), and treatment date. We have no evidence that any information has been subject to actual or attempted misuse as a result of this incident. **Based on our investigation, this event did not impact your financial account numbers or Social Security number.**

What We Are Doing. Information security is among DMG's highest priorities, and we have security measures in place to protect information in our care. Upon becoming aware of this incident, we immediately took steps to confirm the security of our systems. As part of our ongoing commitment to the security of information, we are reviewing existing security policies and have implemented additional cybersecurity measures to further protect against similar incidents from occurring in the future. In addition, we notified law enforcement and are supporting their investigation into this incident.

We are notifying potentially impacted individuals, including you, so that you may take steps to best protect your information, should you feel it is appropriate to do so. We are also reporting this incident to regulatory officials, as required. A special call center has been established by DMG to help answer questions about this incident.

As an added precaution, we are offering you access to credit monitoring and identity theft protection services for 12 months at no cost to you, through Equifax. You may find information on how to enroll in these services in the enclosed "*Steps You Can Take to Protect Your Information.*" We encourage you to enroll in these services as we are not able to do so on your behalf.

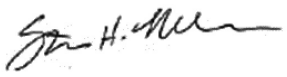
What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed "*Steps You Can Take to Help Protect Personal Information*."

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 800-709-2027 between the hours of 8am and 8pm CST Monday through Friday. This line is staffed with specialists who understand these types of incidents and the steps that can be taken to support you.

DMG will use this incident as an opportunity to continue our aggressive investment in technology and security measures across our enterprise. Our organization shares a restless energy to not only secure our infrastructure but improve every aspect of our technology roadmap to better serve patients. I look forward to sharing more about our efforts as we progress in this journey.

In closing, I want to emphasize my personal ongoing commitment to protect and support every patient we serve. We will work tirelessly to remain your trusted partner in health and care, both now and in the future.

Sincerely,



Steve Nelson
Chief Executive Officer
DuPage Medical Group, Ltd.

Steps You Can Take to Help Protect Personal Information

Enroll in Equifax Credit Watch Gold

EQUIFAX®

Enter your Activation Code: <<*ACTIVATION CODE*>>
Enrollment Deadline: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of <<*ACTIVATION CODE*>> then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

---

[1] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[2] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[3] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com*

[4] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions*

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. DMG is located at 1100 W 31st Street, Downers Grove, IL 60515.

For 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 bureaus 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 violators. 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. We encourage you to 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.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.

DuPage Medical Group Informs Patients of Data Security Incident and Offers Support

August 30, 2021

CHICAGO – Today, DuPage Medical Group (DMG) announced that it identified and addressed a data security incident, and is now notifying patients whose information may have been involved.

On July 13, 2021, DMG experienced a security incident that caused a disruption to its network systems. DMG immediately began working with third-party cyber-forensic specialists to assist in the investigation to determine the full nature and scope of the incident. Through the investigation, it was determined that the network outage was caused by unauthorized actors who gained access to the DMG network, between July 12, 2021, and July 13, 2021. With the assistance of the forensic specialists, DMG conducted a thorough and time-consuming review of its systems to understand whether any patient information may have been impacted as a result of this event. On August 17, 2021, we determined that certain files stored within our environment that contained patient information may have been impacted by this incident.

DMG is in the process of mailing letters to a broad and inclusive list of individuals directly whose information may be involved in this incident. The personal information potentially affected by this included names, addresses, dates of birth, diagnosis codes, CPT codes (Current Procedural Terminology, also known as service codes, are a universal system that identifies medical procedures), and treatment dates. For a small subset of individuals, social security numbers may also have been affected. To date, DMG has no evidence that any information has been subject to actual or attempted misuse as a result of this incident. This event did not impact financial account numbers.

While the investigation determined that only certain portions of the network were impacted by this event, DuPage Medical Group conducted an extensive and thorough investigation and could not rule out the possibility that files containing patients' information may have been impacted by this event.

We take this incident seriously, and as an added precaution, DMG is offering credit monitoring and identify theft protection at no cost for those individuals affected and potentially affected by this incident. A dedicated call center has been established to help address questions. Additional information is available by calling the toll-free incident response line at 1–800–709–2027 between the hours of 8 A.M. and 8 P.M. CST Monday through Friday, or by visiting www.dupagemedicalgroup.com.

future incidents and improve our technology roadmap to better serve patients. Additional details regarding how individuals can protect their information is included below.

Steps You Can Take to Help Protect Personal Information

DMG encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor their credit reports and explanation of benefits forms for suspicious activity. DMG is providing potentially impacted individuals with contact information for the three major credit reporting agencies, as well as providing advice on how to obtain free credit reports and how to place fraud alerts and security freezes on their credit files. The relevant contact information is below:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1−888−766−0008	1−888−397−3742	1−800−680−7289
www.equifax.com	www.experian.com	www.transunion.com

Potentially impacted individuals may also find information regarding identity theft, fraud alerts, security freezes and the steps they may take to protect their information by contacting the credit bureaus, the Federal Trade Commission or their state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1 – 877-ID-THEFT (1−877−438−4338); and TTY: 1−866−653−4261.

Instances of known or suspected identity theft should also be reported to law enforcement or the individual's state Attorney General.

Need Care?

CONTACT US

Corporate Mailing Address
1100 W 31st Street
Downers Grove, Illinois 60515

Main Line - (630) 469-9200
Customer Service - (630) 942-7998

STAY CONNECTED

Sign up for DMG e-Newsletters

Subscribe Now!

Terms of Use

Privacy Policy

ACO

ALSO OF INTEREST:

Clinic Safety

How Parents Can Talk With Their Kids About Coronavirus

We know illness and injury don't consult your schedule.