MEDICAL INFORMATICS ENGINEERING

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

<<mail id>>
<<first name>> <<last name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Re: Notice of Data Security Event

Dear <<First Name>> <<Last Name>>,

My name is Eric Jones and I am co-founder and COO of Medical Informatics Engineering. Our companies provide electronic medical record, patient portal and personal health record services to certain healthcare providers and other clients, including:

<<*Healthcare Provider 1>>
<<*Healthcare Provider 2>>
<<*Healthcare Provider 3>>
<<*Healthcare Provider 4>>
<<*Healthcare Provider 5>>
<<*Healthcare Provider 6>>
<<*Healthcare Provider 7>>
<<*Healthcare Provider 8>>
<<*Healthcare Provider 9>>
<<*Healthcare Provider 10>>

On behalf of Medical Informatics Engineering, I am writing to notify you that a data security compromise occurred at Medical Informatics Engineering that has affected the security of some of your personal and protected health information. This letter contains details about the incident and our response, steps you can take to protect your information, and resources we are making available to help you.

What happened? On May 26, 2015, Medical Informatics Engineering discovered suspicious activity relating to one of its servers. We immediately began an investigation to identify and remediate any identified security vulnerability. Our first priority is to safeguard the security of personal and protected health information, and we are working with a team of third-party forensics experts to investigate the attack and enhance data security and protection. On May 26, 2015, we also reported this incident to law enforcement including the FBI Cyber Squad. Law enforcement is actively investigating this matter, and we are cooperating fully with law enforcement's investigation. The investigation indicates this is a sophisticated cyber attack. Our forensic investigation indicates the unauthorized access to our network began on May 7, 2015.

While investigations into this incident are ongoing, we determined the security of some personal and protected health information contained on Medical Informatics Engineering's network has been affected. The affected data includes your:

<<*Data Element>>	<<*Data Element>>
<<*Data Element>>	<<*Data Element>>
<<*Data Element>>	<<*Data Element>>
<<*Data Element>>	<<*Data Element>>

For additional information on this incident, your affected data, the identity of your affected healthcare provider(s) and the information which came from each of them, if more than one provider is identified above, please call (866) 328-1987.

What we are doing? We take the security of your information very seriously, and apologize for the inconvenience this matter has caused you. Our investigation, the investigation of our third-party data forensics experts, and law enforcement's investigation, are all ongoing. We are also continuing to take steps to remediate and enhance the security of our systems. Remedial efforts include removing the capabilities used by the intruder to gain unauthorized access to the affected systems, enhancing and strengthening password rules and storage mechanisms, increased active monitoring of the affected systems, and intelligence exchange with law enforcement. We have also instituted a universal password reset.

To help protect your identity, we have engaged Experian®, the largest credit bureau in the U.S., to offer you a complimentary two year membership to Experian's ProtectMyID® Elite credit monitoring and identity restoration services. Instructions on how to enroll and receive these services are included in the attached Notice of Privacy Safeguards.

What you can do? We encourage you to enroll and receive the complimentary membership to Experian's ProtectMyID® Elite services we are offering to you. We also encourage you to take steps described in the enclosed Notice of Privacy Safeguards on how to protect yourself against identity theft and fraud.

We recognize that you may have questions that are not answered in this letter. We have established a confidential, toll free hotline to assist you with questions regarding the incident, your affected personal and protected health information, this letter or Experian's identity monitoring and protection services. The hotline can be reached at (866) 328-1987, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, except for holidays. You may also contact Experian directly at (866) 579-4461 for questions regarding the credit monitoring and identity restoration services. You may also visit www.mieweb.com for more information. Updates regarding this incident, our investigation and steps you may take to protect yourself from identity theft and fraud will be available on www.mieweb.com and through our toll free hotline. Questions regarding this letter and the incident should not be directed to your healthcare provider(s) as they may not be able to answer your questions.

We regret any inconvenience this incident may cause. We remain committed to safeguarding the personal and protected health information in our care and will continue to take proactive steps to enhance security.

Sincerely,

Eric Jones
Co-Founder, COO
Medical Informatics Engineering

NOTICE OF PRIVACY SAFEGUARDS

Experian's ProtectMyID® Elite

We encourage you to activate the fraud detection tools available through ProtectMyID® Elite. This product provides you with superior identity protection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

1. ENSURE **That You Enroll By**: 10/25/2015 (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll**: www.protectmyid.com/protect
3. PROVIDE Your Activation Code: [redacted]

If you have questions or need an alternative to enrolling online, please call (866) 579-4461 and provide Engagement number: [redacted] A credit card is not required for enrollment.

You are also able to immediately contact Experian regarding any fraud issues, and have access to the following features once you initiate ProtectMyID:

- **Experian credit report**: See what information is associated with your credit file.
- **Active Surveillance Alerts**: Monitors the Experian file for indicators of fraud.
- **Internet Scan**: Alerts you if your information is found on sites containing compromised data.
- **Address Change Alerts**: Alerts you of changes to your mailing address
- **Fraud Resolution**: Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance**[1]: Provides coverage for certain costs and unauthorized electronic fund transfers.
- **Lost Wallet Protection**: Get help replacing credit, debit, and medical insurance cards.

You may integrate your ProtectMyID membership with the BillGuard app for FREE and receive:

- **Card Fraud Monitoring**: Alerts you when your credit/debit cards are used.
- **Card Concierge**: Resolve billing inquiries and disputes with merchants

If you are a victim of fraud, simply call Experian at (866) 579-4461 by 10/25/2015 and a dedicated Identity Theft Resolution agent will help you restore your identity. Please provide engagement number **PC94878** as proof of eligibility. If you have any questions about ProtectMyID® Elite, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at (866) 579-4461. For additional information on BillGuard you may visit www.protectmyid.com/billguard.

Additional Steps You Can Take to Protect Yourself

In addition to enrolling in Experian's ProtectMyID® Elite, we encourage you to remain vigilant and seek to protect against possible identity theft or other financial loss by regularly reviewing your financial account statements for charges you did not make. We also encourage you to notify your credit card companies, health care providers, and heathcare insurers of this data security incident. You may also review explanation of benefits statement(s) that you receive from your healthcare provider or health plan. If you see any service that you believe you did not receive, you should contact your health care provider or health plan at the telephone number listed on the explanation of benefits statement(s). If you do not receive regular explanation of benefits statement(s), contact your healthcare provider or health plan and ask that they send you a copy after each visit you make to your health care provider.

We also suggest that you carefully review your credit reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

[1]Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Identity protection services

As the investigations continue, and out of an abundance of caution, Medical Informatics Engineering is offering credit monitoring and identity protection services to affected patients, free of charge, for the next 24 months.

Medical Informatics Engineering has established a toll-free call center to answer questions relating to this data security event and the support and services being provided.

Fraud prevention tips

Medical Informatics Engineering suggests that affected patients remain vigilant and seek to protect against possible identity theft or other financial loss by reviewing account statements, notifying their credit card companies, healthcare providers, and insurers of the data compromise, and monitoring their credit reports. Affected patients may also review Explanation of Benefits statements for irregularities. If an individual does not receive regular Explanation of Benefits statements, he or she can contact his or her health plan and request them to send such statements following the provision of services.

Under U.S. law, patients are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

At no charge, potentially affected patients can also have these credit bureaus place a "fraud alert" on their files that alerts creditors to take additional steps to verify their identity prior to granting credit in their names. Please note, however, that because it tells creditors to follow certain procedures to protect the individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms an individual's fraud alert, the others are notified to place fraud alerts on that individual's file. Any individual wishing to place a fraud alert, or who has questions regarding their credit report, can contact any one of the following agencies: Equifax, P.O. Box 105069, Atlanta, GA 30348-5069, 800-525-6285, www.equifax.com; Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/idtheft, or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. State Attorneys General may also have advice on preventing identity theft. Patients can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. For North Carolina residents, the Attorney General can be contacted at