LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS AT LAW

550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

JAMES E. PRENDERGAST
DIRECT DIAL: 215.977.4058
JIM.PRENDERGAST@LEWISBRISBOIS.COM

June 19, 2015

STATE OF NH
DEPT OF JUSTICE
2015 JUN 23 AM 11:06

VIA U.S. MAIL
Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Preliminary Notice of Data Security Event

Dear Attorney General Foster:

We represent Medical Informatics Engineering and NoMoreClipboard, a wholly owned subsidiary of Medical Informatics Engineering, 6302 Constitution Drive, Fort Wayne, Indiana 46804, and are writing to notify you of a data security incident that may have compromised the security of personal information of an as yet unconfirmed number of New Hampshire residents.

Medical Informatics Engineering is a third-party provider that provides electronic medical record services to healthcare providers. NoMoreClipboard provides personal health record/patient portals sponsored by healthcare providers. The affected New Hampshire residents include patients affiliated with certain Medical Informatics Engineering and NoMoreClipboard clients. Medical Informatics Engineering and NoMoreClipboard provided notice of this incident to affected clients on June 2, 2015 in substantially the same form as the letter attached as ***Exhibit A***.

Medical Informatics Engineering and NoMoreClipboard's investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Medical Informatics Engineering and NoMoreClipboard do not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Event

On May 26, 2015, Medical Informatics Engineering discovered suspicious activity in one of its servers. Medical Informatics Engineering immediately began an investigation to identify and remediate any identified security vulnerability. Medical Informatics Engineering is working with a team of third-party experts to investigate the attack and enhance data security and protection. On May 26, 2015, Medical Informatics Engineering also reported this incident to law enforcement including the FBI Cyber Squad.

Law enforcement is actively investigating this matter, and Medical Informatics Engineering is cooperating fully with law enforcement's investigation. The investigation indicates this is a sophisticated cyber attack.

While investigations into this incident are ongoing, Medical Informatics Engineering determined the security of some personal and protected health information contained on Medical Informatics Engineering's network has been affected. The personal and protected health information affected by this incident may include the following information relating to individuals affiliated with certain Medical Informatics Engineering clients: name, mailing address, email address, date of birth, and for some individuals a Social Security number, lab results, dictated reports, and medical conditions. The personal and protected health information affected by this incident relating to affected NoMoreClipboard accounts may include the following information: name, home address, username, hashed password, security question and answer, email address, date of birth, health information, insurance policy information, and Social Security number. No financial or credit card information has been compromised by this incident, as Medical Informatics Engineering and NoMoreClipboard do not collect or store this information.

Notice to Affected New Hampshire Residents

Medical Informatics Engineering and NoMoreClipboard are working to identify the affected New Hampshire residents. While this investigation and law enforcement's investigations continue, Medical Informatics Engineering and NoMoreClipboard are taking appropriate steps to notify individuals potentially affected by this incident. In addition to notifying affected healthcare clients on June 2, 2015, on June 10, 2015, Medical Informatics Engineering and NoMoreClipboard began notifying the public of this security compromise. This notice was posted on Medical Informatics Engineering and NoMoreClipboard's dedicated websites (www.mieweb.com and www.nomoreclipboard.com). A copy of these statements is attached as ***Exhibit B***. Notice of this incident was also distributed by way of press release to major statewide media on June 10, 2015 in substantially the same form as the statement attached here as ***Exhibit C***.

We anticipate that the forensics analysis will be completed shortly. Once the analysis is complete, we will verify the total number of affected individuals, as well as the state of residence for each.

This notice to the New Hampshire Office of the Attorney General will be supplemented accordingly at that time.

Once the third party forensics expert's analysis is complete and the number of affected New Hampshire residents has been confirmed, notice letters will be mailed to the New Hampshire residents for whom Medical Informatics Engineering and NoMoreClipboard have valid mailing addresses pursuant to New Hampshire's data breach notification law. We will also supplement this preliminary notice to your office to provide an update on this data security compromise, the mailing date of notice to the affected New Hampshire residents, and a copy of the notification template that will be used to notify these residents.

Other Steps Taken and To be Taken

Medical Informatics Engineering and NoMoreClipboard take this matter, and the security of the personal and protected health information in its care, seriously and are taking measures to restore the secure functionality of the affected systems. Upon discovering this data security compromise, Medical Informatics Engineering and NoMoreClipboard took steps to identify potential vulnerabilities with its systems, remediate, and enhance the security of its systems. Medical Informatics Engineering and NoMoreClipboard continue to work closely with the third-party experts to identify the nature and scope of this incident and to remediate accordingly. Remedial efforts include removing the capabilities used by the intruder to gain unauthorized access to the Medical Informatics Engineering and NoMoreClipboard affected systems, enhanced and strengthened password rules and storage mechanisms, increased active monitoring of the affected systems, and participating in intelligence exchange with law enforcement. While remediation occurs, Medical Informatics Engineering and NoMoreClipboard have instituted a universal password reset for all affected accounts.

To support potentially affected individuals, Medical Informatics Engineering and NoMoreClipboard established a toll-free hotline to answer questions about this incident and to provide information relating to protection against identity theft and fraud. Medical Informatics Engineering and NoMoreClipboard will provide affected individuals access to a two-year membership to credit monitoring and identity protection services through Experian, at no cost to the affected individual. Medical Informatics Engineering and NoMoreClipboard are also working closely with affected clients to ensure affected individuals are notified of this incident.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security compromise, please contact me at 215-977-4058 or Sian Schafle at 215-977-4067.

Very truly yours,

James E. Prendergast of
LEWIS BRISBOIS BISGAARD & SMITH LLP

SMS:JEP
Encl.

EXHIBIT A

Notice of Medical Informatics Engineering Data Incident

HIPAA Covered Entity:	[name of covered entity]
Number of Individuals:	To be determined
Notice Date:	June 1, 2015
Medical Informatics Engineering Contact:	[name, Title], [telephone number]

Medical Informatics Engineering ("MIE") is writing to provide notice of a data security compromise that may have affected the security of some protected health information contained on our network, relating to certain [client name] patients. We ask that you provide this correspondence to appropriate administrative and/or managerial staff at your company to ensure this incident is brought to the attention of all necessary members of your organization.

On May 26, 2015, the technical team at MIE discovered suspicious activity relating to one of our servers. We immediately initiated our Incident Response Plan and commenced an investigation to identify and remediate any identified security vulnerability. Our team, including independent third-party forensics experts, has been working continuously to understand the nature and scope of the incident and to confirm the security of our systems. This investigation is ongoing. On May 26, 2015, we also reported this incident to the FBI Cyber Squad, and are cooperating with the FBI's investigation.

While our investigation and law enforcement's investigation into this incident are ongoing, we determined that some protected health information contained on our network relating to a soon to be confirmed number of patients was exposed as a result of this incident. The affected data may include patient name, home address, email address, date of birth, and for some patients a Social Security number. Other protected health information affected by this incident may include lab results, dictated reports and medical conditions. Our forensic investigation indicates the unauthorized access to our network occurred on May 7, 2015 through May 8, 2015. The attackers regained unauthorized accessed to our network on May 25, 2015.

We take the security of your patients' information very seriously, and apologize for any concern and inconvenience this may cause you or your patients. Certain legal duties may exist as a result of this exposure, and we would like to assist you in satisfying these duties.

Under applicable law, you may be required to provide notice of this incident to your patients, as well as certain federal and state regulators, and/or the national consumer reporting agencies. We retained Lewis Brisbois Bisgaard & Smith, LLP ("LBBS") to assist us in determining what legal obligations may exist as a result of this incident.

Your company's precise notice obligations, and the time in which you may be required to satisfy such obligations, are determined by HIPAA and potentially various states' laws. Based on your risk assessment, the incident may require you to report details to the U.S. Department of Health and Human Services ("HHS") and to the [client name] patients whose information was contained on our network at the time of the attack. Notification duties to affected individuals, state regulators and the national consumer reporting agencies may also be required under the data breach notification laws of the states where your patients reside. This notice does not constitute legal or compliance advice.

Should you require specific legal guidance, we encourage you to discuss the contents of this letter, and MIE's proposed actions, with independent legal counsel. If you wish to provide notice of this incident to your patients directly, we encourage you to consult legal counsel. LBBS would be happy to discuss this matter with your legal counsel.

We would like to provide notice of this incident, on your company's behalf, to your affected patients, the national consumer reporting agencies, HHS, and applicable State Attorneys General. Attached as ***Exhibit A*** is a list of the regulators MIE will notify regarding this incident. We are notifying only the regulators identified in ***Exhibit A***. If your company has reporting obligations to other regulators, including the California Department of Public Health, that notice will be have to be submitted directly by your company. If you would like MIE to provide notice of this incident to your affected patients, the national consumer reporting agencies, and the regulators identified in ***Exhibit A***, please confirm that we have your authority to provide these notices as soon as possible but, because time is of the essence, no later than [DATE]. [**FOR applicable clients requiring system review: We also need your authority to access your company's data contained on our network to determine the identity of the affected [client name] patients and the precise protected health information relating to these individuals that has been affected by this incident**]. Consent to provide these notices on your company's behalf may be sent to [Eric Jones contact information].

We take the security of protected health information very seriously. With your authorization, in addition to mailing notice to your affected patients, we will also provide your affected patients with the opportunity to enroll in identity monitoring and protection services at no cost to them should they feel it is appropriate to do so.

We will establish a toll-free number that individuals can call if they have any questions regarding this incident. That number will be provided in the notices to affected individuals.

We are continuing to investigate this incident, and we are working diligently to address any identified security vulnerability associated with this incident. We are also reviewing our security practices to enhance the security of protected health information at MIE.

All questions regarding this notice and questions regarding the provision of mailing addresses should be directed to our privacy and data security counsel, James Prendergast at (215) 977-4067.

Our investigation into this incident is ongoing. We will update you with any substantial developments in this matter. We remain committed to the privacy of protected health information, and sincerely regret any inconvenience or concern that this may have caused you.

Sincerely,

[signatory]
[title]

Notice of Medical Informatics Engineering Data Incident

HIPAA Covered Entity:	[name of covered entity]
Number of Individuals Impacted:	To be determined
Notice Date:	June 1, 2015
NMC/Medical Informatics Engineering Contact:	[name, Title], [telephone number]

NoMoreClipboard ("NMC") is writing to provide notice of a data security compromise that may have affected the security of some protected health information relating to certain individuals who used a NMC patient portal/personal health record sponsored by your organization. We ask that you provide this correspondence to appropriate administrative and/or managerial staff at your company to ensure this incident is brought to the attention of all necessary members of your organization.

On May 26, 2015, the technical team at our parent company (Medical Informatics Engineering) discovered suspicious activity relating to one of its servers. We immediately initiated our Incident Response Plan and commenced an investigation to identify and remediate any identified security vulnerability. Our team, including independent third-party forensics experts, has been working continuously to understand the nature and scope of the incident and to confirm the security of our systems. This investigation is ongoing. On May 26, 2015, we also reported this incident to the FBI Cyber Squad, and are cooperating with the FBI's investigation.

While our investigation and law enforcement's investigation into this incident are ongoing, we determined that some protected health information contained on our network, including information relating to a soon to be confirmed number of individuals who used a NMC portal sponsored by your organization, was exposed as a result of this incident. The affected data may include patient name, home address, email address, date of birth and Social Security number. No financial or credit card information was compromised, as we do not collect or store this information. Our forensic investigation indicates the unauthorized access to our network occurred on May 7, 2015 through May 8, 2015. The attackers regained unauthorized accessed to our network on May 25, 2015.

[Our investigation thus far indicates that patient records from your Medical Informatics Engineering electronic health record have not been compromised.]

Comment [SS1]: For NMC clients who also have MIE eHR

We take the security of your patients' information very seriously, and apologize for any concern and inconvenience this may cause you or your patients. Certain legal duties may exist as a result of this exposure, and we would like to assist you in satisfying these duties.

Under applicable law, you may be required to provide notice of this incident to your patients, as well as certain federal and state regulators, and/or the national consumer reporting agencies. We retained Lewis Brisbois Bisgaard & Smith, LLP ("LBBS") to assist us in determining what legal obligations may exist as a result of this incident.

Your company's precise notice obligations, and the time in which you may be required to satisfy such obligations, are determined by HIPAA and potentially various states' laws. Based on your

risk assessment, the incident may require you to report details to the U.S. Department of Health and Human Services ("HHS") and to the [client name] patients whose information was contained on our network at the time of the attack. Notification duties to affected individuals, state regulators and the national consumer reporting agencies may also be required under the data breach notification laws of the states where your patients reside. This notice does not constitute legal or compliance advice.

Should you require specific legal guidance, we encourage you to discuss the contents of this letter, and NMC's proposed actions, with legal counsel. If you wish to provide notice of this incident to your patients directly, we encourage you to consult legal counsel. LBBS would be happy to discuss this matter with your legal counsel.

NMC would like to provide notice of this incident, on your company's behalf, to your affected patients, the national consumer reporting agencies, HHS, and applicable State Attorneys General. Attached as ***Exhibit A*** is a list of the regulators NMC will notify regarding this incident. We are notifying only the regulators identified in ***Exhibit A***. If your company has reporting obligations to other regulators, including the California Department of Public Health, that notice will have to be submitted directly by your company. If you would like NMC to provide notice of this incident to your affected patients, the national consumer reporting agencies, and the regulators identified in ***Exhibit A***, please confirm that we have your authority to provide these notices as soon as possible but, because time is of the essence, no later than **Friday, June 12, 2015.** Consent to provide these notices on your company's behalf may be sent to [Eric Jones contact information].

NMC takes the security of protected health information very seriously. With your authorization, in addition to mailing notice to your affected patients, we will also provide your affected patients with the opportunity to enroll in identity monitoring and protection services at no cost to them should they feel it is appropriate to do so.

We will establish a toll-free number that individuals can call if they have any questions regarding this incident. That number will be provided in the notices to affected individuals.

We are continuing to investigate this incident, and we are working diligently to address any identified security vulnerability associated with this incident. We are also reviewing our security practices to enhance the security of protected health information at NMC.

All questions regarding this notice and questions regarding the provision of mailing addresses should be directed to our privacy and data security counsel, James Prendergast at (215) 977-4067.

Our investigation into this incident is ongoing. We will update you with any substantial developments in this matter. We remain committed to the privacy of protected health information, and sincerely regret any inconvenience or concern that this may have caused you. .

Medical Informatics Engineering Notifies Individuals of a Data Security Compromise

Fort Wayne, Indiana, June 10, 2015 – On behalf of itself and its affected clients, Medical Informatics Engineering is writing to provide notice of a data security compromise that has affected the security of some protected health information relating to certain patients affiliated with certain Medical Informatics Engineering clients. *We emphasize that the patients of only certain clients of Medical Informatics Engineering were affected by this compromise and those clients have all been notified.* Clients include: Concentra, Fort Wayne Neurological Center, Franciscan St. Francis Health Indianapolis, Gynecology Center, Inc. Fort Wayne, and Rochester Medical Group.

On May 26, 2015, Medical Informatics Engineering discovered suspicious activity relating to one of its servers. Medical Informatics Engineering immediately began an investigation to identify and remediate any identified security vulnerability. Medical Informatics Engineering's team, including independent third-party forensics experts, has been working continuously to investigate the attack and enhance data security and protection. On May 26, 2015, Medical Informatics Engineering also reported this incident to law enforcement including the FBI Cyber Squad. Law enforcement is actively investigating this matter, and Medical Informatics Engineering is cooperating with law enforcement's investigation. Medical Informatics Engineering's forensic investigation indicates the unauthorized access to our network began on May 7, 2015. The investigation indicates this is a sophisticated cyber attack.

Compromised information

While investigations into this incident are ongoing, Medical Informatics Engineering determined the security of some protected health information contained on Medical Informatics Engineering's network has been affected. The protected health information affected by this incident relates to patients affiliated with certain Medical Informatics Engineering clients identified above and may include the patients' name, mailing address, email address, date of birth, and for some patients a social security number, lab results, dictated reports, and medical conditions. No financial or credit card information has been compromised, as we do not collect or store this information.

Medical Informatics Engineering also determined that this cyber attack compromised protected health information for its NoMoreClipboard subsidiary. Separate notice is being issued for affected clients and patients associated with NoMoreClipboard.

Notification

On June 2, 2015, Medical Informatics Engineering began contacting and mailing notice letters disclosing this incident to affected Medical Informatics Engineering clients.

Affected patients for whom Medical Informatics Engineering has a valid postal address will be notified of this incident through U.S. mail. Medical Informatics Engineering will also be disclosing this incident to certain state and federal regulators.

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 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For

Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Kentucky residents, the Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601-3449, 502-696-5389, www.ag.ky.gov.

Toll-free hotline

To better assist those who may potentially have been affected, Medical Informatics Engineering has established a confidential, toll-free hotline to answer questions. This hotline is available Monday through Friday, 9:00 a.m. to 9:00 p.m. E.T., and can be reached at (866) 328-1987. Updates will be posted to this website.

We take the security of health information very seriously and understand that such incidents cause real concern. We apologize sincerely and thank our customers for their continued loyalty and patience as we work through this challenge.

Massachusetts residents can click here for additional information.

NoMoreClipboard Notice to
Individuals of a Data Security Compromise

Fort Wayne, Indiana, June 10, 2015 On behalf of itself and its affected clients, NoMoreClipboard is writing to provide notice of a data security compromise that has affected the security of some protected health information relating to certain clients and individuals who have used a NoMoreClipboard personal health record or patient portal.

On May 26, 2015, we discovered suspicious activity in one of our servers. We immediately began an investigation to identify and remediate any identified security vulnerability. Our first priority is to safeguard the security of patient health information, and we are working with a team of third-party experts to investigate the attack and enhance data security and protection. This investigation is ongoing. 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.

Information Compromised

While investigations into this incident are ongoing, we determined that the security of some protected health information contained in NoMoreClipboard accounts has been affected. The affected data relating to individuals who used a NoMoreClipboard portal/personal health record may include an individuals' name, home address, username, hashed password, security question and answer, email address, date of birth, health information, and Social Security number. No financial or credit card information has been compromised, as we do not collect or store this information. Our forensic investigation indicates the unauthorized access to our network began on May 7, 2015. At this time we are working to quantify the number of patients affected by this incident.

We strongly encourage all NoMoreClipboard users to change their passwords. We also strongly encourage everyone to use different passwords for each of their various accounts. Do not use the same password twice. The next time a NoMoreClipboard user logs in, we will prompt a password change. As part of the password change process, users will be sent a 5 digit PIN code to either a cell phone, via an automated phone call, or to an email address already associated with the NoMoreClipboard account. Users will have to enter this 5 digit code to reset their password. We are also emailing NoMoreClipboard users to encourage this password change.

Notification

On June 2, 2015, we began contacting and mailing notice letters disclosing this incident to affected NoMoreClipboard clients.

Affected individuals for whom we have a valid postal address will also be notified of this incident through U.S. mail. We will also be disclosing this incident to certain state and federal regulators.

Identity protection services

As the investigations continue, and out of an abundance of caution, we are offering credit monitoring and identity protection services to affected individuals, free of charge, for the next 24 months.

We have 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

We suggest that affected individuals 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 individuals 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, individuals 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 individuals 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. Individuals 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 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor,

Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Kentucky residents, the Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601-3449, 502-696-5389, www.ag.ky.gov.

Toll-free hotline

To better assist those who may potentially have been affected, we have established a confidential, toll-free hotline to answer questions. This hotline is available Monday through Friday, 9:00 a.m. to 9:00 p.m. E.T., and can be reached at (866) 328-1987. Updated will be posted to this website.

We take the security of health information very seriously and understand that such incidents cause real concern. We apologize sincerely and thank our customers for their continued loyalty and patience as we work through this challenge.

Massachusetts residents can click here for additional information.

EXHIBIT C

PRESS CONTACT: MELANIE THOMAS
mthomas@informtheagency.com
202-390-7887

STATEMENT REGARDING MEDICAL INFORMATICS ENGINEERING'S RECENT CYBER ATTACK

A Message from Eric Jones
Co-Founder & COO, Medical Informatics Engineering
June 10, 2015

A sophisticated cyber attack has compromised some of the protected health information contained on our Medical Informatics Engineering and NoMoreClipboard networks. As soon as we detected suspicious activity on May 26, we launched an internal investigation, retained independent third-party forensics experts, and alerted law enforcement, including the FBI Cyber Squad. Our initial investigation indicates that the unauthorized access to our network began on May 7, 2015.

Our first priority is to safeguard the security of patient health information. We are working with a team of IT security experts to investigate the attack and enhance data security and protection.

Affected data includes names, addresses, dates of birth, social security numbers and other protected health information. No financial or credit card information has been compromised, as we do not collect or store that information.

We are working diligently to determine how many patients were affected by this incident, and we have notified affected healthcare provider clients and business associates. Individuals will be notified by letter if their information was compromised.

We are offering credit monitoring and identity protection services to affected individuals, free of charge, for the next 24 months. We have also established a toll-free call center to answer questions about this attack and the support and services being provided.

We take the security of health information very seriously and understand that such incidents cause real concern. We apologize sincerely and thank our customers for their continued loyalty and patience as we work through this challenge.

For more information, please contact the toll-free call center at 866-328-1987.

Medical Informatics Engineering notifies
Patients of a Data Security Compromise

Fort Wayne, Indiana, June 10, 2015 – On behalf of itself and its affected clients, Medical Informatics Engineering is writing to provide notice of a data security compromise that has affected the security of some protected health information relating to certain patients affiliated with certain Medical Informatics Engineering clients. *We emphasize that the patients of only certain clients of Medical Informatics Engineering were affected by this compromise and those clients have all been notified.* Clients include: Concentra, Fort Wayne Neurological Center, Franciscan St. Francis Health Indianapolis, Gynecology Center, Inc. Fort Wayne, and Rochester Medical Group.

On May 26, 2015, Medical Informatics Engineering discovered suspicious activity relating to one of its servers. Medical Informatics Engineering immediately began an investigation to identify and remediate any identified security vulnerability. Medical Informatics Engineering's team, including independent third-party forensics experts, has been working continuously to investigate the attack and enhance data security and protection. On May 26, 2015, Medical Informatics Engineering also reported this incident to law enforcement including the FBI Cyber Squad. Law enforcement is actively investigating this matter, and Medical Informatics Engineering is cooperating with law enforcement's investigation. Medical Informatics Engineering's forensic investigation indicates the unauthorized access to our network began on May 7, 2015. The investigation indicates this is a sophisticated cyber attack.

Compromised information

While investigations into this incident are ongoing, Medical Informatics Engineering determined the security of some protected health information contained on Medical Informatics Engineering's network has been affected. The protected health information affected by this incident relates to patients affiliated with certain Medical Informatics Engineering clients identified above and may include the patient's name, mailing address, email address, date of birth, and for some patients a social security number, lab results, dictated reports, and medical conditions. No financial or credit card information has been compromised, as we do not collect or store this information.

Medical Informatics Engineering also determined that this cyber attack compromised protected health information for its NoMoreClipboard subsidiary. Separate notice is being issued for affected clients and patients associated with NoMoreClipboard.

Notification

On June 2, 2015, Medical Informatics Engineering began contacting and mailing notice letters disclosing this incident to affected Medical Informatics Engineering clients.

Affected patients for whom Medical Informatics Engineering has a valid postal address will be notified of this incident through U.S. mail. The same information contained in the notice letter will also be available at the Medical Informatics Engineering website – www.mieweb.com. Medical Informatics Engineering will also be disclosing this incident to certain state and federal regulators.

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

9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Kentucky residents, the Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601-3449, 502-696-5389, www.ag.ky.gov.

Toll-free hotline

To better assist those who may potentially have been affected, Medical Informatics Engineering has established a confidential, toll-free hotline to answer questions. This hotline is available Monday through Friday, 9:00 a.m. to 9:00 p.m. E.T., and can be reached at (866) 328-1987. Affected patients can also visit www.mieweb.com for additional information and updates.

We take the security of health information very seriously and understand that such incidents cause real concern. We apologize sincerely and thank our customers for their continued loyalty and patience as we work through this challenge.

NoMoreClipboard Notice to
Individuals of a Data Security Compromise

Fort Wayne, Indiana, June 10, 2015 On behalf of itself and its affected clients, NoMoreClipboard is writing to provide notice of a data security compromise that has affected the security of some protected health information relating to certain clients and individuals who have used a NoMoreClipboard personal health record or patient portal.

On May 26, 2015, we discovered suspicious activity in one of our servers. We immediately began an investigation to identify and remediate any identified security vulnerability. Our first priority is to safeguard the security of patient health information, and we are working with a team of third-party experts to investigate the attack and enhance data security and protection. This investigation is ongoing. 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.

Information compromised

While investigations into this incident are ongoing, we determined that the security of some protected health information contained in NoMoreClipboard accounts has been affected. The affected data relating to individuals who used a NoMoreClipboard portal/personal health record may include an individuals' name, home address, username, hashed password, security question and answer, email address, date of birth, health information, and Social Security number. No financial or credit card information has been compromised, as we do not collect or store this information. Our forensic investigation indicates the unauthorized access to our network began on May 7, 2015. At this time we are working to quantify the number of patients affected by this incident.

We strongly encourage all NoMoreClipboard users to change their passwords. We also strongly encourage everyone to use different passwords for each of their various accounts. Do not use the same password twice. The next time a NoMoreClipboard user logs in, we will prompt a password change. As part of the password change process, users will be sent a 5 digit PIN code to either a cell phone, via an automated phone call, or to an email address already associated with the NoMoreClipboard account. Users will have to enter this 5 digit code to reset their password. We are also emailing NoMoreClipboard users to encourage this password change.

Notification

On June 2, 2015, we began contacting and mailing notice letters disclosing this incident to affected NoMoreClipboard clients.

Affected individuals for whom we have a valid postal address will also be notified of this incident through U.S. mail. The same information contained in the notice letter will also be available at www.NoMoreClipboard.com. We will also be disclosing this incident to certain state and federal regulators.

Identity protection services

As the investigations continue, and out of an abundance of caution, we are offering credit monitoring and identity protection services to affected individuals, free of charge, for the next 24 months.

We have 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

We suggest that affected individuals 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 individuals 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, individuals 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 individuals 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. Individuals 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

9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Kentucky residents, the Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601-3449, 502-696-5389, www.ag.ky.gov.

Toll-free hotline

To better assist those who may potentially have been affected, we have established a confidential, toll-free hotline to answer questions. This hotline is available Monday through Friday, 9:00 a.m. to 9:00 p.m. E.T., and can be reached at (866) 328-1987. Affected individuals can also visit www.NoMoreClipboard.com for additional information and updates.

We take the security of health information very seriously and understand that such incidents cause real concern. We apologize sincerely and thank our customers for their continued loyalty and patience as we work through this challenge.