McDonald Hopkins
A business advisory and advocacy law firm®

STATE OF NH
DEPT OF JUSTICE
2016 MAR 14 AM 11:50

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Dominic A. Paluzzi
Direct Dial: 248.220.1356
dpaluzzi@mcdonaldhopkins.com

March 7, 2016

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: eClinicalWorks – Incident Notification

Dear Attorney General Delaney:

McDonald Hopkins PLC represents eClinical Works, LLC located in Westborough, Massachusetts. I write to provide notification concerning an incident that affects the security of personal information of nine (9) New Hampshire residents. eClinicalWorks' investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, eClinicalWorks does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On February 22, 2016, as a result of a phishing email received by an eClinicalWorks employee appearing to come from a company executive, an unauthorized third party received an electronic file containing certain information on eClinicalWorks' current and former employees. The email requested employees' 2015 W-2 tax forms, which were sent to the unauthorized email account. The employee immediately realized the error and notified eClinicalWorks executives.

Upon learning of the issue, eClinicalWorks' incident response team promptly launched an investigation, including reporting the incident to law enforcement. As part of its investigation, eClinicalWorks has been working very closely with external cybersecurity professionals who regularly investigate and analyze these types of incidents.

We have confirmed that the information that was received by the unauthorized party included employees' names, Social Security numbers, home addresses, salary, and tax withholding information. No information from spouses or dependents was included in the file sent

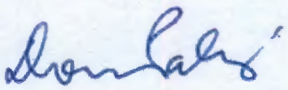
As a result, eClinicalWorks wanted to notify you (and the affected residents) about this incident and explain the services they are making available to safeguard residents against identity fraud. eClinicalWorks provided the New Hampshire residents with written notice of this incident commencing on March 7, 2016, in substantially the same form as the letter attached

hereto. eClinicalWorks has advised the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. eClinicalWorks is also offering the residents a complimentary five-year membership with a credit monitoring and identity theft protection service and is providing dedicated call center support to answer questions. eClinicalWorks has advised the residents about the process for placing a fraud alert on their credit files, placing a security freeze, obtaining a free credit report, and the process for reporting identity theft to the IRS. The residents have also been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

eClinicalWorks takes its obligation to protect personal information very seriously. eClinicalWorks is continually evaluating and modifying its practices to enhance the security and privacy of personal information, including training its workforce on security threats.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,



Dominic A. Paluzzi

DAP/kjb
Encl.

eClinicalWorks
2 Technology Drive
Westborough, MA 01581

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

<<mail id>>
<<Name1>>
<<Name2>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name 1>>,

The privacy of your personal information is of utmost importance to eClinicalWorks. I am writing with important follow-up information about a recent incident involving the security of our employees' personal information. We wanted to provide you with additional information regarding the incident and explain the services we are making available to safeguard you against identity fraud. We are also providing additional steps you can take to further protect your information.

What Happened?

On February 22, 2016, as a result of a phishing email received by one of our employees appearing to come from me, an unauthorized third party received an electronic file containing certain information on our current and former employees. The email requested our employee's 2015 W-2 tax forms, which were sent to the unauthorized email account. The employee immediately realized the error and notified me.

What Information Was Involved?

We have confirmed that the information that was received by the unauthorized party included your full name, Social Security number, home address, salary, and tax withholding information. No information from your spouse or dependents was included in the file sent.

What We Are Doing.

Upon learning of the issue, our incident response team promptly launched an investigation, including reporting the incident to law enforcement. As part of our investigation, we have been working very closely with external cybersecurity professionals who regularly investigate and analyze these types of incidents. We wanted to continue to keep you updated on this incident, explain the services we are making available to safeguard you against identity fraud, and suggest steps that you should take as well.

What You Can Do.

Enclosed you will find information on enrolling in a **5-year** membership in AllClear PRO TBO from AllClear ID, which is a three-bureau option credit monitoring and identity theft resolution service that we are providing at no cost to you. We have also included information about other precautionary measures you can take to protect your personal information, including placing a Fraud Alert, placing a Security Freeze and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis. In the event that you determine that there has been fraudulent activity on any of your accounts, you should promptly notify the financial institution or organization that maintains the impacted account.

As a reminder, always verify the email address and sender of any email you receive requesting confidential or sensitive information. If you have any doubt about a request for confidential information, you should contact the apparent requestor via telephone or in person to confirm the request.

For More Information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 877-615-3740. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Saturday, 9:00 a.m. to 9:00 p.m. Eastern Time.

On behalf of eClinicalWorks, please accept my sincere apologies that this incident occurred. We are committed to maintaining the privacy of your information and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your information, including training our workforce on security threats. Please know that we are devoting considerable resources to ensure our employees are fully informed and protected as a result of this unfortunate incident.

Sincerely,

Girish Kumar Navani
Chief Executive Officer
eClinicalWorks, LLC

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 5-Year Credit Monitoring and Identity Theft Restoration Services.

Protecting your personal information is important to eClinicalWorks. As an added precaution, we have arranged to have AllClear ID protect your identity for **5 years** at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 5 years.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 877-615-3740 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear PRO TBO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO TBO service, you will need to provide your personal information to AllClear ID. You may sign up online at **enroll.allclearid.com** or by phone by calling 877-615-3740 using the following redemption code: **<<Account Code>>**.

Please note: Additional steps may be required by you in order to activate your phone alerts and triple bureau monitoring options.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 60 month credit monitoring services, we recommend that you place an initial 90-day "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	**Experian**	**TransUnion**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

3. Consider 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. 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, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
PO Box 105788	PO Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-685-1111	1-888-397-3742	1-800-680-7289

The Federal Trade Commission (FTC) also has additional information about security alerts and security freezes available at: https://www.identitytheft.gov/.

4. 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.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the 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.

6. Reporting Identity Fraud to the IRS.

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you do the following:

- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf
- Call the IRS at (800) 908-4490 to report the situation.

Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 60 months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 60 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period.
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company.
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft;

Coverage under AllClear Secure Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur; and
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud;
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of Secure coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077