McDonald Hopkins
A business advisory and advocacy law firm®

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

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

July 30, 2018

**VIA E-MAIL; consumer@ag.iowa.gov; Susan.Kerr@ag.iowa.gov**

Ms. Susan M. Kerr
Consumer Protection Division Security
Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

**Re: UnityPoint Health – Incident Notification**

Dear Ms. Kerr:

McDonald Hopkins PLC represents UnityPoint Health. I write to provide notification regarding an incident that may involve the protected health information and/or personal information of 960,561 Iowa residents. UnityPoint Health's 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, UnityPoint Health does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

On May 31, 2018, UnityPoint Health discovered that a phishing email attack had compromised its business email system which may have resulted in unauthorized access to protected health information and other personal information for some patients. Upon learning of this attack, UnityPoint Health informed law enforcement agencies and launched an investigation with an expert computer forensics firm to determine the size and scope of the attack, as well as the number of people potentially impacted.

The investigation shows that UnityPoint Health received a series of fraudulent phishing emails which tricked some employees into providing their confidential sign-in information which gave attackers access to their internal email accounts between March 14, 2018 and April 3, 2018. While unauthorized access to patient information may have occurred, no known or attempted misuse of patient information has been reported at this time. Electronic medical record and patient billing systems were not impacted by this attack. The only unauthorized access to patient information may have occurred through compromised email accounts, where the information was contained in the body of an email or in attachments such as reports.

Patient information that may have been in compromised email accounts included patient names and one or more of the following: addresses, dates of birth, medical record numbers,

medical information, treatment information, surgical information, diagnoses, lab results, medications, providers, dates of service and/or insurance information. For some individuals, information may have included a Social Security number and/or driver's license number. For a limited number of individuals, information may also have included payment card or bank account numbers.

UnityPoint Health has taken a number of important steps intended to prevent similar situations from happening in the future, including password resets for all compromised accounts to prevent further unauthorized access, implemented mandatory education for employees to help them recognize and avoid phishing emails, added technology to identify suspicious external emails; and implemented multi-factor authentication.

UnityPoint Health is providing written notification via U.S. Mail commencing on July 30, 2018 to individuals impacted by this incident (where last known home address was available), in substantially the same form as the letter attached hereto. UnityPoint Health will offer free credit monitoring services for one year to individuals whose Social Security number and/or driver's license number were included in the compromised email accounts. UnityPoint Health will advise the residents to remain vigilant in reviewing account and explanation of benefits statements for fraudulent or irregular activity. UnityPoint Health will provide dedicated call center support to answer questions. Where applicable, UnityPoint Health will advise the residents about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. Where applicable, the residents will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

In addition, we have notified the Secretary of the U.S. Department of Health and Human Services Office for Civil Rights, pursuant to 45 CFR 164.408.

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.

Notification Response Center
PO Box 6336
Portland, OR 97228-6336

***IMPORTANT INFORMATION***
***PLEASE READ CAREFULLY***

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

<<Date>>

Dear <<Name 1>>:

UnityPoint Health values our relationship with every patient, and maintaining your trust and confidence is important to us. Therefore, we are sorry to inform you about an incident that impacts you and your information. On May 31, 2018, we discovered that a phishing email attack had compromised our business email system and may have resulted in unauthorized access to protected health information and other personal information for some patients. Our investigation indicates that some of your information was contained in one or more of the compromised email accounts.

We take our responsibility to protect your information seriously and deeply regret this incident occurred. While we are not aware of any misuse of patient protected health or other personal information, we want to inform you about what happened, what information was involved, what we have done to address the situation, and what you can do to help protect yourself.

**What Happened**

Our investigation shows that our organization received a series of fraudulent emails known as "phishing" that were disguised to appear to have come from a trusted executive within our organization. The phishing emails tricked some of our employees into providing their confidential sign-in information which gave attackers access to their internal email accounts between March 14, 2018 and April 3, 2018. Some of the compromised accounts included emails or attachments to emails, such as standard reports related to healthcare operations, containing protected health information and/or personal information for certain patients. While unauthorized access to patient information may have occurred, no known or attempted misuse of patient information has been reported at this time.

Our investigation and outside experts' review indicate that this series of phishing emails was part of an attack on our business email system. According to computer forensic experts and law enforcement, these types of attacks are usually financially motivated. The phishing attack on UnityPoint Health was more likely focused on diverting business funds from our organization, rather than on obtaining patient information. Based on our investigation, we believe the perpetrators were trying to use the email system to divert payroll or vendor payments.

We want to reassure you that our electronic medical record and patient billing systems were not impacted by this attack. The only unauthorized access to patient information may have occurred through compromised email accounts, where the information was contained in the body of an email or in attachments such as reports. It is common and appropriate for patient information to be shared through business email between employees authorized to use it as part of their work to support patient care.

**What Information Was Involved**

The compromised email account(s) that were accessed may have included your name and one or more of the following information: address, date of birth, Social Security number, driver's license number, medical record number, medical information, treatment information, surgical information, diagnosis, lab results, medication(s), provider(s), date(s) of service, insurance information, payment card number and/or bank account number.

**What UnityPoint Health Has Done to Address the Situation**

Upon learning of this attack, UnityPoint Health launched an investigation with an expert computer forensics firm to determine the size and scope of the attack, as well as the number of people potentially impacted. We informed law enforcement agencies about this situation. In addition, our organization has taken a number of important steps intended to prevent similar situations from happening in the future:

- We reset passwords for all compromised accounts to prevent further unauthorized access;
- We conducted mandatory education for our employees to help them recognize and avoid phishing emails;
- We added technology to identify suspicious external emails; and
- We implemented multi-factor authentication which requires users to go through multiple steps to verify their identity in order to access our systems.

**What You Can Do to Protect Your Personal and Health Information**

We want to help protect you from potential misuse of your personal information. We are offering you a free one-year membership for credit monitoring through Experian IdentityWorks℠ Credit 3B. This service helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your one-year membership, please see the additional information provided in this letter.

Also enclosed, you will find information about other precautionary measures you can take, including placing a fraud alert and/or security freeze on your credit files and obtaining a free credit report. Additionally, we encourage you to remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis. You should also review your payment card account statements closely and report any unauthorized charges to your card issuer immediately because card-network rules generally provide that cardholders are not responsible for unauthorized charges that are reported promptly. The phone number to call is usually on the back of the payment card.

Finally, we want to make you aware of what you can do to protect your medical identity by monitoring your health information:

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your health insurance company, HMO or health benefits provider for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

**For More Information**

**If you have any questions or concerns regarding this incident, please call our dedicated and confidential toll-free helpline at 1-888-266-9285.** The help line is staffed by professionals familiar with this incident and knowledgeable about what you can do to protect against misuse of your information. The help line is available Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time. Information is also available on our website at ***www.unitypoint.org/security-notice***.

Finally, please accept our sincere apology for this incident. UnityPoint Health is committed to protecting your information and has many procedures in place to help safeguard it. We are continually evaluating and modifying our security practices to further strengthen the privacy of your personal and health information.

Sincerely,

RaeAnn Isaacson
Privacy Officer UnityPoint Health

**– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –**

**1. Enrolling in Complimentary 12-Month Credit Monitoring**

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

**Activate IdentityWorks Credit 3B Now in Three Easy Steps**

1. ENROLL by: **<<Enrollment Date>>** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll at [redacted]
3. PROVIDE the **Activation Code**: **<<Activation Code>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted] Be prepared to provide engagement number **<<Engagement #>>** as proof of eligibility for the identity restoration services by Experian.

**ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:**

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at [redacted]**
**or call [redacted] to register with the activation code above.**

**What you can do to protect your information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, 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 [redacted]

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** 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.

## 2. Placing a Fraud Alert

You may 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 19016 |
| 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

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. 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 19016 |
| https://www.freeze.equifax.com | http://experian.com/freeze | http://www.transunion.com/securityfreeze |
| 1-800-685-1111 | 1-888-397-3742 | 1--888-909-8872 |

## 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 Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

**Iowa Residents**: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164.