UnityPoint Health

NOTICE REGARDING SECURITY INCIDENT

UnityPoint Health values our relationship with every patient, and maintaining trust and confidence is important to us. On May 31, 2018, UnityPoint Health discovered that a phishing email attack had compromised its business email system and 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.

We take our responsibility to protect patient information seriously and deeply regret this incident occurred. While we are not aware of any misuse of patient information related to this incident, we are notifying patients about what happened, what information was involved, what we have done to address the situation, and what patients can do to help protect their information.

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.

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

Patient information that may have been contained 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.

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 federal 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.

UnityPoint Health mailed notification letters via U.S. Mail on July 30, 2018, to individuals impacted by this incident (where last known home address was available).

What Impacted Patients Can Do to Protect Their Personal and Health Information

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. If eligible, instructions on how to enroll are included in the notification letters mailed to impacted patients' last known home address.

Below is information about other precautionary measures impacted individuals can take, including placing a fraud alert and/or security freeze on credit files and obtaining a free credit report if Social Security number and/or driver's license number are impacted. Additionally, we encourage impacted individuals to remain vigilant in reviewing their financial account statements for fraudulent or irregular activity on a regular basis. If payment card information was impacted, payment card account statements should be reviewed closely and any unauthorized charges should be reported to the 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, impacted patients can protect their medical identity by monitoring their health information:

- Only share health insurance cards with health care providers and other family members who are covered under the insurance plan or who help with medical care.
- Review "explanation of benefits statements" which are received from the health insurance company. Follow up with the insurance company or care provider for any items that are not recognized. 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 the health insurance company, HMO or health benefits provider for a current year-to-date report of all services paid as a beneficiary. Follow up with the insurance company or the care provider for any items not recognized.

For More Information

For patients who have questions or concerns regarding this incident, or to determine if they are impacted by this incident, UnityPoint Health has established a dedicated and confidential toll-free helpline at 1-888-266-9285. The helpline is staffed by professionals familiar with this incident and knowledgeable about what patients can do to protect against misuse of their information. The helpline is available Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time.

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

Below is information about other precautionary measures impacted individuals can take, including placing a fraud alert and/or security freeze on credit files and obtaining a free credit report, if Social Security number and/or driver's license number are impacted

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
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

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
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111

Experian Security Freeze
PO Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1--888-909-8872

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.

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: 515-281-5926.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.