Security Notice Frequently Asked Questions

What happened?

UnityPoint Health received a series of "phishing" emails that compromised its business email system and may have resulted in unauthorized access to protected health information and other personal information for some patients. Phishing is the use of fraudulent email to trick recipients into providing access to personal or protected information. The series of phishing emails sent to UnityPoint Health employees was disguised to appear to have come from a trusted executive, tricking some employees into providing their confidential sign-in information which gave attackers access to their internal email accounts from March 14 to April 3, 2018. On May 31, 2018, we discovered that some of the compromised accounts included emails or attachments to emails containing protected health information and other personal information for some patients.

Why was my information in an employee email account?

It is common and appropriate for reports containing patient information to be shared through business email between employees who are authorized to use it for their work. Business reports are created for variety of purposes, including to track payments from patients' primary insurance carriers or to contact patients regarding follow-up appointments.

How do I know if my information was accessed?

Our investigation identified which email accounts were compromised and what types of information were included in the compromised accounts. However, it is not always possible to know whether the information was viewed by the attacker. While unauthorized access to patient information may have occurred, we are not aware of any misuse of this information at this time. However, it is important that you take steps to protect your health and personal information as recommended in the notification above or the letter you received.

Did attackers access my medical record?

UnityPoint Health's medical record system was not impacted by the phishing email attack. Only the business email system was impacted.

Did attackers access my billing information?

UnityPoint Health's patient billing system was not involved in the phishing email attack. Only the business email system was impacted. However, some billing information may have been contained in reports within compromised email accounts

Who is UnityPoint Health?

UnityPoint Health is a Midwest health system with hospitals, clinics and other services in Iowa, Illinois and Wisconsin.

Why did UnityPoint Health have my information?

Because you are or were a patient at a UnityPoint Health hospital or clinic, some of your health and personal information is on file with the organization for billing, insurance and other purposes related to your care.

What has UnityPoint Health 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 officials about this situation. In addition, our organization has taken a number of important steps intended to prevent similar situations from happening in the future:

- Passwords were reset for all compromised accounts to prevent further unauthorized access;
- Mandatory education was conducted for employees to help them recognize and avoid phishing emails;
- Technology was added to identify suspicious external emails; and
- Multi-factor authentication, which requires users to go through multiple steps to verify their identity in order to access systems, is now required.

How do I know if I'm affected?

On July 30, letters were sent to impacted individuals at their last known home address, if available. If you received a notification letter and have questions, or to determine if you may be affected, you may call our toll-free help line 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 a.m. to 8 p.m. Central Time.

What information was involved?

After a detailed forensic investigation and document review, UnityPoint Health determined that protected health information was contained in compromised email accounts, including patient names and one or more of the following: dates of birth, medical record numbers, 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 driver's license number. For a limited number of individuals, information may also have included credit card or bank account information.

When did the phishing attack occur?

Our investigation determined that the compromised accounts may have been accessed between March 14, 2018 and April 3, 2018. After discovering the issue, UnityPoint Health promptly took action to secure the compromised email accounts and changed passwords.

What has the unauthorized person(s) done with my information?

To date, we are not aware of any reports of identity fraud, identity theft, or improper use of patient information as a result of this incident. However, we want to make you aware of the situation so you can take precautionary measures to protect your information.

As a result of this incident, will I become a victim of identity theft?

Not necessarily. To date, we are not aware of any reports of identity fraud, identity theft, or improper use of information as a result of this incident. However, we want to make you aware of the situation so you can take precautionary measures to protect your information.

What steps has UnityPoint Health taken to secure its systems and prevent this from happening again?

UnityPoint Health has taken a number of important steps intended to protect its systems and prevent similar situations from happening in the future. Specific actions include:

- Resetting passwords for all compromised accounts to prevent further unauthorized access;
- Conducting mandatory education for employees to help them recognize and avoid phishing emails;

- Adding technology to identify suspicious external emails; and
- Implementing multi-factor authentication which requires users to go through multiple steps to verify their identity in order to access systems.

How can I protect my medical/health/insurance information?

UnityPoint Health has no information to date indicating that your protected health information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft:

- 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 the care provider for any items you don't 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 (March 14, 2018 through April 3, 2018) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow-up with your insurance company or care provider for any items you don't recognize.

Are there any reports of actual misuse of the information as a result of this incident?

To date, we are not aware of any reports of identity fraud, identity theft, or improper use of patient information as a result of this incident. However, we want to make you aware of the situation so you can take precautionary measures to protect your information.

Has the unauthorized person who accessed the email accounts been identified or caught?

UnityPoint Health does not have any knowledge that the person or persons who accessed the email accounts have been identified or caught.

Has law enforcement been notified about this incident?

Yes. Upon learning of the attack, law enforcement agencies were notified.

How is this incident related to the incident announced in April?

In April, UnityPoint Health notified approximately 16,400 patients of a separate phishing email attack. Law enforcement agencies report dramatic increases in attacks on business email systems. Often carried out by international criminal organizations, these highly sophisticated attacks utilize complex schemes that are constantly evolving.

Why isn't free credit monitoring being offered to everyone affected?

For some affected individuals, information may have included a Social Security number and driver's license number. For other individuals, only medical, health, or insurance information was affected, so their Social Security number and/or driver's license number were not at risk. Since a credit monitoring service does not track activity related to medical, health or insurance information, credit monitoring would not be an effective way to track that information. Instead, experts recommend several steps these individuals can take to monitor their protected 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 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 and remain vigilant in reviewing your account statements regularly for fraudulent or irregular activity.

My letter indicates that my credit card or bank account number was impacted. What should I do?

You should review your payment card and financial account statements closely and report any unauthorized charges to the card issuer or banking institution 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. You may also contact your banking institution to determine if you should change your account number(s).

How do I enroll in the free credit monitoring service?

Enrollment instructions for eligible individuals can be found in the notification letter received in the mail, utilizing the 9-character Activation Code included in the letter. Further instructions for enrolling are contained in your notification letter. The deadline to enroll is November 1, 2018. A credit card is not required to enroll.