UnityPoint Health

Amy Varcoe, Media Relations
UnityPoint Health
C: 515-491-8813
Amy.Varcoe@unitypoint.org

NEWS RELEASE – FOR IMMEDIATE RELEASE

UNITYPOINT HEALTH NOTIFIES PATIENTS OF SECURITY INCIDENT

(WEST DES MOINES, Iowa – July 30, 2018) UnityPoint Health announced today that it has notified approximately 1.4 million patients of a recent email phishing incident that may have compromised certain patient protected health or personal information.

"We take our responsibility to protect patient information very seriously and deeply regret this incident occurred," said RaeAnn Isaacson, Privacy Officer, UnityPoint Health. "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."

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.

The forensics investigation revealed that UnityPoint Health received a series of fraudulent emails known as "phishing" that were disguised to appear to have come from a trusted executive within the organization. The phishing emails 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. 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.

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. While unauthorized access to patient information may have occurred, no known or attempted misuse of patient information has been reported as a result of this incident at this time.

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 encourages impacted individuals to remain vigilant in reviewing account statements for fraudulent or irregular activity on a regular basis, including a review of any "explanation of benefits statements". Individuals should follow up with the applicable insurance company or care provider for any items that are not recognized.

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. Business reports are created for a variety of purposes, including to track payments from patients' primary insurance carriers or to contact patients regarding follow-up appointments.

According to computer forensic experts and law enforcement, these types of phishing email attacks are usually financially motivated. The phishing attack on UnityPoint Health was more likely focused on diverting business funds like payroll or vendor payments, rather than on obtaining patient information.

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.

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.

"We continue to work closely with leading experts to learn from our experience and help our organization – and other health care organizations – prevent these kinds of cybercrimes," said Isaacson.

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). UnityPoint Health has also notified the news media and posted notices on the homepages of the health system website and all affiliate websites.

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. In addition, UnityPoint Health has established a dedicated website (www.unitypoint.org/security-notice) where patients can access information regarding the incident, including frequently asked questions and tips for protecting their information.

# # #

About UnityPoint Health

UnityPoint Health is the nation's 13th largest nonprofit health system and the fourth largest nondenominational health system in America, providing care throughout Iowa, western Illinois and southern Wisconsin.