MU Health Care Reports Second Phishing Attack of the Year

By Steve Alder

Published: 2020-09-29 · Archived: 2026-04-05 19:38:39 UTC

Posted By on Sep 29, 2020

University of Missouri Health Care (MU Health Care) has experienced a phishing attack that saw several employee email accounts compromised between May 4 and May 6, 2020. An investigation into the breach revealed the compromised email accounts contained patient information including names, account numbers, dates of birth, health insurance information, Social Security numbers, and driver's license numbers.

MU Health Care has notified all patients affected by the attack and has offered individuals whose Social Security number was potentially compromised complimentary credit monitoring services. No reports have been received that suggest any patient information has been misused. Two breach reports have been submitted to the HHS' Office for Civil Rights (OCR) about email-related data breaches, one on June 11, 2020, involving the protected health information of 5,074 patients, and another on September 17, 2020, involving the protected health information of 189,736 individuals. MU Health also reported an email breach last year on August 2, 2024, involving the protected health information of 14,402 patients.

Data Leaked Following University Hospital SunCrypt Ransomware Attack

University Hospital, a teaching hospital in Newark, NJ, has experienced a ransomware attack involving SunCrypt ransomware. The attack occurred in September 2020. Prior to the use of ransomware, the attackers exfiltrated around 48,000 documents, some of which were published on the ransomware operator's data leak site.

It is unclear at this stage how many patients have been affected by the breach, but the leaked data did include some patient data, including names, dates of birth, Social Security numbers, driver's license numbers, and other data.

THE HIPAA JOURNAL READER OFFER

Get The FREE
HIPAA Compliance Checklist

Immediate Delivery of Checklist Link To Your Email Address

Please Enter Correct Email Address

Your Privacy Respected

HIPAA Journal Privacy Policy

The attack appears to have started with a phishing email that resulted in the TrickBot Trojan being downloaded. SunCrypt ransomware was delivered as a secondary payload.

University Hospital has confirmed that a ransom of $640,000 was paid to the attackers for the keys to decrypt files and to prevent 240 GB of data from being published.

PHI of 4,806 Patients Potentially Compromised in UCare Minnesota Phishing Attack

The non-profit health plan, UCare Minnesota, has experienced a phishing attack involving several employee email accounts. An investigation was launched into a suspected breach when suspicious network activity was detected in April 2020. On May 4, 2020, UCare Minnesota determined certain email accounts had been accessed by an unauthorized individual. The email accounts were immediately secured and were subjected to a review to determine whether member information had been accessed.

UCare Minnesota learned on September 1, 2020, that the email accounts contained the personal and protected health information of 4,806 individuals, including names, birth dates, healthcare provider names, diagnosis information, and health insurance ID numbers.

No evidence was found to suggest any information was exfiltrated or misused by the individuals responsible for the attack. UCare Minnesota has since re-educated employees on phishing attacks and has bolstered email security.

Nebraska Medicine Suffers Cyberattack

Nebraska Medicine has announced it has suffered a cyberattack that has taken its computer systems out of action. The cyberattack occurred on Sunday, September 25, 2020, resulting in an outage that caused “significant information technology system downtime.”

Without access to critical IT systems, Nebraska Medicine was forced to postpone appointments for patients who were due to have elective procedures or had other non-emergent health concerns. Medicine issued a statement on September 24 stating normal operations would resume “in days”. The emergency room remained open and no ER patients were diverted to alternate facilities.

It is unclear whether patient records were accessed or stolen in the attack, but Nebraska Medicine confirmed that no patient records were deleted or destroyed and that all patient data could be recovered from backups.

Source: https://www.hipaajournal.com/mu-health-care-phishing-attack-impacts-5000-patients/