CYBERSECURITY AND DATA PRIVACY

INFORMATION MEMO

NOVEMBER 30, 2023

Ransomware Attack on Ardent Health Services Causes Disruption at Hospitals in Six Different States

On Nov. 27, 2023, Nashville-based healthcare corporation Ardent Health Services (Ardent) announced that a ransomware attack impacted 30 of its hospitals and forced the shutdown of several emergency rooms in at least three states. This announcement came days after the U.S. Cybersecurity and Infrastructure Security Agency (CISA) notified Ardent of suspicious activity in its environment.

Over Thanksgiving weekend, Ardent launched an investigation into the network activity and notified law enforcement. Ardent also engaged third-party forensic and threat intelligence advisers to investigate the breach and assist with restoring its information technology operations. On Nov. 23, investigators were able to confirm the suspicious activity was a ransomware attack.

To contain the threat, Ardent has taken its network offline and suspended access to its information technology applications for all users, including its corporate servers, Epic software, internet and clinical programs. As a result, many non-urgent elective surgeries will be rescheduled after Ardent's network is restored. As of November 28, half of Ardent's 25 emergency rooms were diverting patients requiring immediate care to other local hospitals. To date, Ardent has not commented on whether health records or financial information have been compromised.

Key Takeaways

The ransomware attack on Ardent demonstrates the real-time severity of impact that cyberattacks targeting large health care organizations can have on the patients they serve. A health care provider's sudden loss of data can create ripple effects that impact a patient's ability to receive medical care for weeks or even months after a threat has been contained. Further, a recent study showed that during a ransomware attack, in-hospital mortality increases by 20-25%. Health care companies should take steps to preserve the integrity of data by creating frequent backups of sensitive records that are stored on a separate and secure network.

Ardent's unfortunate incident is not an anomaly. Hospitals and other healthcare facilities remain a high-value target for cybercriminals due to these organizations' large troves of sensitive data, and heavy reliance on technology to provide critical patient care, including maintenance of electronic health records necessary for physicians to rely upon for patient evaluation and diagnosis. Just this year, several other health care organizations throughout the country have suffered similar cyberattacks. For example, Nevada-based medical transportation company Perry Johnson & Associates experienced a cyberattack that impacted two healthcare providers in New York State. During the breach, Social Security numbers and medical information were accessed by the cybercriminal. This prompted New York Attorney General Letitia James to warn affected New York residents to take preventative action against identity theft.

Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters. If you have any questions about the information presented in this memo, please contact Jessica Copeland, CIPP/US, Mario Ayoub or any attorney in Bond's cybersecurity and data privacy practice.

**Special thanks to Associate Trainee Victoria Okraszewski for her assistance in the preparation of this blast. Victoria is not yet admitted to practice law.*

BOND SCHOENECK & KING ATTORNEYS