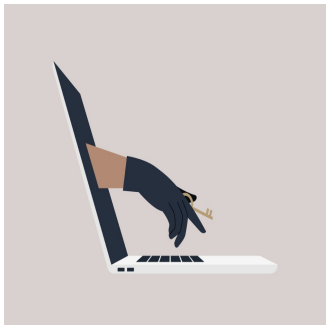
HealthManagement
Promoting Management and Leadership

Ascension Restores Digital Health Records Following Ransomware Attack



Ascension has announced the full restoration of its digital patient records across all hospitals and healthcare locations, marking a significant recovery milestone after a recent ransomware attack. The breach, which occurred due to an employee inadvertently downloading a malicious file, had severely impacted patient care and operational efficiency since it was first discovered on May 8.

Impact on Patient Care and System Recovery

The health system, which operates 140 hospitals and numerous clinics across 19 states and Washington, D.C., reported that as of Friday morning, all its facilities have regained full access to their electronic health records. This development is expected to enhance clinical workflows, appointment scheduling, and prescription fulfilment, restoring operations to their pre-attack state. Despite this progress, Ascension acknowledges that the restoration of some systems is still underway, and the investigation into the breach is ongoing.

The cyberattack had led to significant disruptions, including the diversion of ambulances, longer patient wait times, and the postponement of non-emergency procedures. Some information collected during the downtime may not be immediately available, and patient portal responses might still experience delays due to high volumes.

Identifying the Breach Source

Ascension has identified the breach's source as a malicious file downloaded by an employee. While the organisation believes this was an honest mistake, the attackers managed to access files from seven of Ascension’s approximately 25,000 servers. These files potentially contain private health information and other identifying data. The health system is currently analysing the extent of the exposed information and has not found evidence that data from electronic health records or clinical systems was compromised.

Response and Mitigation Efforts

In response to the attack, Ascension is collaborating with law enforcement and cybersecurity experts to investigate and enhance its security measures. The organization is also providing credit monitoring and identity theft protection services to patients and staff potentially affected by the breach. These efforts aim to mitigate any potential damage and reassure those affected.

The incident underscores the vulnerability of the healthcare sector to cyberattacks. Cybersecurity experts, including Keith Forrester of Optiv, highlight the need for better employee training on cybersecurity practices, as phishing remains a primary entry point for ransomware. Forrester notes that attackers are using increasingly sophisticated methods, often leveraging AI tools to create convincing phishing emails.

Ascension's experience is part of a broader trend of escalating cyberattacks on healthcare organizations. In 2023 alone, over 100 million Americans were affected by such incidents. The recent ransomware attack on Change Healthcare is a notable example, impacting hospitals and healthcare providers nationwide. As Ascension continues to bolster its defenses and support affected individuals, the incident serves as a stark reminder of the critical importance of cybersecurity in protecting patient data and maintaining the integrity of healthcare operations.

Source Credit: ChiefHealthcareExecutive
Image Credit: iStock

Published on : Thu, 20 Jun 2024

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.