Indiana Executive Council on Cybersecurity

IECC Quarterly Healthcare Newsletter – Q1 2025

IN THE SPOTLIGHT

DaVita discovered a ransomware attack on 12 April, which encrypted parts of its network, causing operational disruptions across its more than 2,600 facilities. The attack highlights vulnerabilities where cybercriminals target healthcare networks to disrupt access to critical systems like electronic health records. Authorities have not disclosed specific details of the attack's cause and associated threat actors, but the incident underscores the persistent threat of ransomware in the healthcare sector and the need for effective cybersecurity strategies.

Local Healthcare Cybersecurity News

Becker's Health IT reported about the Indiana Executive Council on Cybersecurity's Healthcare Cyber in a Box 2.1 initiative, designed to support smaller providers with cybersecurity resources sourced from larger systems. The program offers free downloads with cybersecurity guidance at basic, intermediate, and mature levels, focusing on protecting vulnerable smaller health organizations from cyber threats. Healthcare Cyber in a Box 3.0 will soon release, featuring a front-page alert with immediate steps for organizations suspecting of a cyberattack or incident.

Industry Trends

Healthcare Breaches Drop in Q1, Compliance Challenges Persist: The Department of Health and Human Services Office for Civil Rights reported a significant drop in healthcare data breaches in March, down 46% from last year and marking a continued decrease during the past three months. Despite this decrease, hacking and IT incidents remain the primary cause, accounting for 79% of breaches, largely originating from network servers and compromised email accounts. In March 2025, healthcare providers reported 45 data breaches affecting 1,733,464 individuals, health plans had 5 breaches affecting 18,911, and business associates documented 3 breaches impacting 1,722 individuals. Additionally, the OCR took enforcement actions against Oregon Health & Science University and Health Fitness Corporation for HIPAA violations, resulting in penalties of $200,000 and $227,816, respectively, highlighting ongoing compliance challenges.

Healthcare Data Breaches Continue Amid Growing Ransomware Threats: *HIPAA Journal* reported a persistent rise in healthcare data breaches over the past 14 years, with 2023 setting records at 725 incidents exposing over 133 million records. Causes have shifted from theft to hacking and ransomware, which comprised nearly 80% of breaches in 2023. Despite digital safeguards, ransomware attacks rose 278% since 2018. Early estimates for 2024 originally forecasted fewer breaches, however, compromised records surged to 275 million due to the Change Healthcare attack affecting 190 million individuals. OCR's investigation backlog remains due to funding issues.

Local Events

- IECC Healthcare Virtual Cyber Clinic
  - Tuesday, June 24th (Save the Date-More Details to Come Soon)

- Public-Sector Cybersecurity Summit: 18 June at the Embassy Suites by Hilton Noblesville
- Indianapolis CISO Executive Summit: 28 October at the Sheraton City Center

Healthcare Cybersecurity Resources

- IECC's Healthcare Cyber in a Box 2.1 provides cybersecurity guidance for basic, intermediate, and mature business maturity levels, offering actionable advice on email, system, and device protections to address specific threats and support Hoosiers and small to medium-sized businesses.
- The Department of Health and Human Services provides cybersecurity guidance to help HIPAA-covered entities and business associates report cyber-related security incidents.
- The HHS 405(d) Program collaborates with the Health Sector Coordinating Council to enhance cybersecurity practices in the Healthcare and Public Health sector, offering resources, tools, and best practices to educate and drive behavioral change, ultimately strengthening the sector's cybersecurity posture against evolving threats.
- The Centers for Disease Control and Prevention offers cybersecurity resources, including guides, training materials, and protective strategies for public health systems and data.
- The Cybersecurity and Infrastructure Security Agency offers a healthcare cybersecurity toolkit incorporating risk-mitigation best practices and a framework for accessing and improving cyber resiliency.
- The NIST Cybersecurity Framework (CSF), created by the National Institute of Standards and Technology, is a voluntary guide that helps organizations manage cybersecurity risks through a structured approach. It offers standards and best practices focused on six key functions: Govern, Identify, Protect, Detect, Respond, and Recover.

Please contact David Ayers at: dayers@iot.in.gov for inquiries or to share your healthcare cybersecurity story or incident for potential inclusion in future quarterly newsletters. Anonymity is optional.