Briefings on HIPAA

Cybersecurity on the mind: Key takeaways for HIPAA security officers from recent HHS reports

by Dom Nicastro

HHS released two reports recently that provide in-depth insights and compliance tips to help healthcare covered entities contend with cybersecurity threats.

The reports came out of the HHS 405(d) program—a collaborative initiative between the private security sector and federal government—and are aimed at aligning healthcare industry security practices to bolster cybersecurity across the sector. This program focuses on providing useful resources, tools, and products to organizations nationwide in order to enhance their cybersecurity posture against threats.

Let's dive into the highlights from these two reports and get some compliance tips from the security experts.

First report: Hospital Cyber Resiliency Initiative Landscape Analysis

This report aims to provide a detailed analysis of current cybersecurity threats within the healthcare sector and corresponding protective measures; in particular, it focuses on cyber resiliency to ensure the continuous delivery of care amid cyberthreats.

The report is structured to help healthcare organizations, especially hospitals, understand their cybersecurity capabilities and preparedness—it guides them on resource allocation for the best protection against cyberthreats.

A highlight of the report's key features include:

- **Threat analysis:** The report conducts a thorough examination of active threats targeting hospitals.
- **Capabilities assessment:** The report assesses participating hospitals' cybersecurity capabilities and readiness, benchmarking against the Health Industry Cybersecurity Practices (HICP).
- **Best practices identification:** The report identifies best practices using data from a diverse mix of hospital types and geographies.
- **Methodology:** The report incorporates multiple sources of data, including threat data from the U.S. government, cybersecurity vendors, open-source intelligence, and quantitative analyses of major survey instruments. It also includes conversations with geographically and demographically diverse hospitals.
- **Collaborative effort:** The report contains contributions from various government entities, vendors, and cybersecurity groups, demonstrating a multistakeholder approach.
- **Outcome:** By providing a clear understanding of the cybersecurity landscape, the report aims to guide healthcare organizations, including HIPAA security officers and other stakeholders, in investing their time and resources to better protect against cybersecurity threats.

Here are some more takeaways from the report HIPAA security officers should note:

- **Definition of cyber resiliency:** The report outlines the concept of cyber resiliency as defined by the National Institute of Standards and Technology (NIST). This encompasses the ability to anticipate, withstand, recover from, and adapt to adverse cyber conditions—an essential set of tools for maintaining patient care and safety.
- **Benchmarking against HICP:** The analysis was benchmarked against the HICP to evaluate current cybersecurity capabilities and readiness across participating hospitals.
- **Thorough data analysis:** Utilizing data from various sources like the U.S. government, cybersecurity vendors, and open-source intelligence, the report conducts a quantitative analysis of cybersecurity capabilities. This extensive analysis can aid in understanding prevalent threats and the effectiveness of current cybersecurity measures.
- **Real-world case studies:** By incorporating real-world statistics and case studies, the report offers practical insights into areas where time and resources are needed to bolster cybersecurity.
- **Active threat analysis:** The report's authors conducted a thorough review of active threats targeting hospitals to better understand the landscape of cybersecurity threats. This analysis can help in preparing for and mitigating these threats.
- **Focus on patient care and safety:** The report concentrates on activities that protect access to patient care and safety, providing a clear focus on minimizing the impact of cyberthreats on clinical operations.
- **Sharing findings with HSCC CWG:** One of the objectives was to share the report's findings with the Health Sector Coordinating Council Cyber Working Group (HSCC CWG) for consideration. This sharing of information can help in prioritizing cybersecurity practices for U.S. hospitals.

© 2023 HCPro, a division of Simplify Compliance LLC.

Second report: Five key insights from the Healthcare Cybersecurity Benchmarking Study

The second report, also provided by the HHS 405(d) program, aims to provide information on cybersecurity practices in the healthcare sector. It is designed to broaden awareness and align healthcare security approaches.

Here are some takeaways from the report HIPAA security officers should note:

- **Medical device security concerns:** There's a significant disparity in adoption of various industry best practices, according to the study. While email protections rank the highest in adoption, medical device security lags behind with just over 50% coverage. Given the rapid growth of the internet of medical things and the increasing number of network-connected medical devices, this area requires urgent attention, especially with ransomware groups posing direct threats to patient care and safety.
- **Role of the CISO in medical device security:** A notable correlation was found between chief information security officer (CISO) program ownership and HICP adoption for medical device security. When the CISO's office took responsibility for medical device security, there was an 18% increase in HICP coverage.
- **National Cybersecurity Strategy Implementation Plan:** The White House released a new National Cybersecurity Strategy Implementation Plan, detailing over 65 high-impact federal initiatives. These initiatives range from combating cybercrimes to building a skilled cyber workforce. The HHS 405(d) program encourages healthcare stakeholders to familiarize themselves with this plan.
- **Supply chain risk management:** Supply chain risk management ranks last in relative maturity across all 23 NIST Cybersecurity Framework categories. Managing third-party risk remains a challenge due to its manual and time-consuming nature. The largest healthcare breach in 2022 was a result of a hacking incident at a printing and mailing vendor, affecting 2.7 million individuals across 37 healthcare delivery organizations.
- **Cybersecurity insurance recommendations:** Cyberinsurance can help protect businesses against losses from cyberattacks. However, it's essential to ensure that the policy covers various cyberthreats, including data breaches, cyberattacks on vendor data, nation-state attackers, insider threats, and ransomware attacks. It's also crucial to determine if the insurance provider offers defense in lawsuits or regulatory investigations and provides a breach hotline.
- **Privacy and security risks from online tracking technologies:** The Office for Civil Rights and the Federal Trade Commission have issued warnings to hospital systems and telehealth providers about the potential privacy and security risks posed by online tracking technologies.

Cybersecurity Q&A with Anurag Lal

In light of the HHS reports, we caught up with Anurag Lal, CEO of NetSfere, for a Q&A on cybersecurity best practices.

Q: What proactive measures can healthcare organizations implement to identify and mitigate cyberthreats before they escalate?

A: In order to mitigate cyberthreats, healthcare organizations must adopt strong cybersecurity strategies to protect their business, their data, and their bottom line. Reducing cyber risk requires enterprises to adopt technologies aligned with zero-trust principles, consistently train employees on cybersecurity, and establish security-first bring-your-own-device policies.

When implementing technology into the workplace, it's essential that it has a zero-trust security posture. Healthcare organizations' weakest links can also be having employees who are not trained in cybersecurity awareness. Verizon's 2022 Data Breach Investigations Report found that 82% of breaches involved the "human element." Training employees on the importance of data security and how to recognize cyberattacks equips them with the knowledge to identify suspicious activities. With consistent security training, employees will stay updated on company security protocols such as changing passwords often and helping them remain on the alert for evolving malware, phishing, and social engineering attacks.

In addition to employee training, healthcare enterprises should enforce an acceptable use policy for bringing their own devices. To avoid a potential data breach, the policies that should be enforced include requiring passwords with multifactor authentication, requiring employees to use VPNs when working remotely, and prohibiting the downloading of unsanctioned apps and the use of unauthorized messaging apps in workflows.

Q: How can healthcare organizations transition from a reactive to a proactive cybersecurity approach?

A: Many healthcare organizations don't prioritize compliance and run the risk of hefty fines, lawsuits, loss of revenue, reputational damage, and loss of consumer trust. Many cybercriminals target healthcare enterprises to gain access to protected health information.

To transition from a reactive approach to a proactive one, healthcare organizations can implement technologies that are HIPAA, GDPR, and FINRA compliant. Today, fines for HIPAA violations range from $127 to $50,000 per violation depending on the nature of the violation. Healthcare organizations must make sure their technologies are compliant, on top of ensuring employees are aware of any potential risks.

© 2023 HCPro, a division of Simplify Compliance LLC.

Healthcare enterprises need to choose the right technology partners and solutions. Enterprises can build and sustain digital trust, reaping the benefits of fewer privacy breaches and cybersecurity incidents, stronger customer loyalty and patient care, and higher revenue, by creating a zero-trust model for their company.

Q: How can healthcare organizations align their cybersecurity strategies with the National Cybersecurity Strategy Implementation Plan?

A: Healthcare organizations need to execute digital resilience in order to align cybersecurity strategies. The organization must read, understand, and implement the newest plans so that employees can mitigate and avoid cyberthreats and promote transparency for patients and the enterprise. As enterprises begin to align with this plan, healthcare business leaders will now give its security measures more thought, recognizing if anything is outdated or at risk.

Q: What role do federal initiatives play in shaping the cybersecurity landscape for healthcare providers?

A: Federal initiatives act as a guideline for healthcare providers about what to look out for, what to prepare for, and how to adjust their cybersecurity landscape. Healthcare systems should heed them with diligence.

Q: What are the emerging cybersecurity threats that healthcare organizations should be aware of, and how can they prepare for them?

A: Digital transformation is still expanding, more specifically in artificial intelligence. Healthcare organizations are adopting this tool to provide fast service to patients online, assist employees with internal questions, and help with threat detection systems.

While this technology can be useful, it also plays a role in committing data breaches and jeopardizing patient safety and the financial health of an organization. In addition, it provides solutions or outcomes based on the information it is given. Healthcare organizations must know if the technology is consistent with the company's policies, as well as if it's compliant and the information is legally obtained.

Sharing private health data and using AI is a serious concern. The best way to prepare for this emerging trend is through end-to-end encrypted technology. Establishing safe and secure platforms will enhance the safety of the organization and patient information.

"Except where specifically encouraged, no part of this publication may be reproduced, in any form or by any means, without prior written consent of HCPro, or the Copyright Clearance Center at 978-750-8400. Opinions expressed are not necessarily those of RCA. Mention of products and services does not constitute endorsement. Advice given is general, and readers should consult professional counsel for specific legal, ethical, or clinical questions."

© 2023 HCPro, a division of Simplify Compliance LLC.