Topic Disposition: Cybersecurity Impacts on Healthcare Topic Nomination

Date: 5/25/2024
Nomination Number: 1045

Purpose: This document summarizes the information addressing a nomination submitted on April 14, 2023, (link to nomination) through the Effective Health Care Website. This information was used to inform the Evidence-based Practice Center (EPC) Program decisions about whether to produce an evidence report on the topic, and if so, what type of evidence report would be most suitable.

Issue: The nominator is interested in improvements to protection from cyber-attacks in the US healthcare system. Specifically, they are interested in increasing measurements of cybersecurity rating scores to better track cybersecurity effectiveness.

Findings: The EPC Program will not develop a new evidence product because the nomination is outside of the program's scope.

Background

Modern healthcare systems are dependent on connected technical systems consisting of many medical devices and hardware, software, and networking tools. The ability of these complex systems to communicate and cooperate with one another is essential for modern healthcare delivery. Connectivity and interoperability are also requirements of the Meaningful Use provision of the Health Information Technology for Economic and Clinical Health Act of 2009.[1] As advanced as these systems are, they are also rife with vulnerabilities.

Cybersecurity is the art and science of protecting networks, devices, and data from unauthorized access or criminal use, and the practice of ensuring confidentiality, integrity, and availability of information. Among the many cybersecurity risks facing health care systems in the US, concern for impacts on patient outcomes are the greatest. A few of the most concerning threats are dangers associated with increased patient morbidity & mortality,[2] malware erasing or disabling entire systems at point of care, attackers breaking into systems and altering patient or other electronic records, or attackers stealing financial information.[3]

Healthcare systems are a profitable target for hackers, and the healthcare sector has historically lagged in cybersecurity compared with many other sectors, including retail and finance.[4] The Privacy Rights Clearinghouse, a nonprofit organization based in the US, reported that there were more than 20,000 data breaches between 2005 and 2022.[5] The total number of records exposed in these breaches exceeded 20 billion. The healthcare sector, which includes medical insurance services, represented the majority (37%) of those data breaches.[5] For the 13th year in a row, IBM Security's 2023 data breach report found that the US healthcare data breach cost was the highest

average cost of any industry, coming in at $10.93 million. IBM's report found that healthcare industry breach costs had risen 53% since 2020.[5]

Related Resources

We identified additional resources which may of interest:

- The Office of Civil Rights: https://www.hhs.gov/hipaa/for-professionals/breach-notification/reports-congress/index.html
- The Health Sector Cybersecurity Coordination Center: https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html#threat-briefs
- The Office of the National Cyber Director (ONCD): The National Cybersecurity Strategy[6]

References

1. HITECH Act of 2009, 42 USC sec 139w-4(0)(2) (February 2009), part 2, subtitle C, sec 13301, subtitle B, sec 3014: Competitive grants to States and Indian tribes for the development of loan programs to facilitate the widespread adoption of certified EHR technology
2. McGlave, Claire and Neprash, Hannah and Nikpay, Sayeh, Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients (October 4, 2023). Available at SSRN: https://ssrn.com/abstract=4579292 or http://dx.doi.org/10.2139/ssrn.4579292
3. What is Cybersecurity? | CISA. Cybersecurity and Infrastructure Security Agency CISA. Published February 1, 2021. https://www.cisa.gov/news-events/news/what-cybersecurity
4. Choi SJ, Johnson ME. The relationship between cybersecurity ratings and the risk of hospital data breaches. J Am Med Inform Assoc. 2021 Sep 18;28(10):2085-2092. doi: 10.1093/jamia/ocab142. PMID: 34338786; PMCID: PMC8449620.
5. Cost of a data breach 2023 | IBM. https://www.ibm.com/reports/data-breach
6. Joe Biden. *NATIONAL CYBERSECURITY STRATEGY*.; 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

---

Conflict of Interest: None of the investigators have any affiliations or financial involvement that conflicts with the material presented in this report.

This report was developed by the Scientific Resource Center under contract to the Agency for Healthcare Research and Quality (AHRQ), Rockville, MD (Contract No. HHSA 75Q80122C00002). The findings and conclusions in this document are those of the author(s) who are responsible for its contents; the findings and conclusions do not necessarily represent the views of AHRQ. No statement in this article should be construed as an official position of the Agency for Healthcare Research and Quality or of the U.S. Department of Health and Human Services.

Persons using assistive technology may not be able to fully access information in this report. For assistance contact EPC@ahrq.hhs.gov.