

Enhancing Healthcare Data Protection and Security

Authors : Joseph Udofia, Isaac Olufadewa

Abstract : Everyday, the size of Electronic Health Records data keeps increasing as new patients visit health practitioner and returning patients fulfil their appointments. As these data grow, so is their susceptibility to cyber-attacks from criminals waiting to exploit this data. In the US, the damages for cyberattacks were estimated at \$8 billion (2018), \$11.5 billion (2019) and \$20 billion (2021). These attacks usually involve the exposure of PII. Health data is considered PII, and its exposure carry significant impact. To this end, an enhancement of Health Policy and Standards in relation to data security, especially among patients and their clinical providers, is critical to ensure ethical practices, confidentiality, and trust in the healthcare system. As Clinical accelerators and applications that contain user data are used, it is expedient to have a review and revamp of policies like the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Fast Healthcare Interoperability Resources (FHIR), all aimed to ensure data protection and security in healthcare. FHIR caters for healthcare data interoperability, FHIR caters to healthcare data interoperability, as data is being shared across different systems from customers to health insurance and care providers. The astronomical cost of implementation has deterred players in the space from ensuring compliance, leading to susceptibility to data exfiltration and data loss on the security accuracy of protected health information (PHI). Though HIPAA hones in on the security accuracy of protected health information (PHI) and PCI DSS on the security of payment card data, they intersect with the shared goal of protecting sensitive information in line with industry standards. With advancements in tech and the emergence of new technology, it is necessary to revamp these policies to address the complexity and ambiguity, cost barrier, and ever-increasing threats in cyberspace. Healthcare data in the wrong hands is a recipe for disaster, and we must enhance its protection and security to protect the mental health of the current and future generations.

Keywords : cloud security, healthcare, cybersecurity, policy and standard

Conference Title : ICCSA 2024 : International Conference on Cybersecurity and Security Analysis

Conference Location : New York, United States

Conference Dates : January 29-30, 2024