The implications of patient data security considerations for EHR interoperability and downtime recovery

TREO Talk Paper

Utkarsh Shrivastava  
Western Michigan University  
Utkarsh.shrivastava@wmich.edu

Carrie Song  
Western Michigan University  
carrie.song@wmich.edu

Bernard Han  
Western Michigan University  
bernard.han@wmich.edu

Abstract

The ransomware attacks on healthcare organizations increased threefold in 2017 contributing to a collective loss of about US $6 billion to the healthcare industry. These attacks often lead to Electronic Health Record (EHR) system outages resulting in system downtime and delaying patient care. Another area of concern for the healthcare organizations is the lack of interoperability of EHR systems leading to data errors which oftentimes culminates to a mistaken identity of a patient posing a greater health risk. The interoperability of EHR arises due to inability of information systems, devices or other applications within the healthcare organization to connect in a coordinated way for a meaningful and efficient use of patient’s medical data. In order to realize the benefits of the EHR adoption hospitals strive for a seamless sharing and integration of patient information through hospital process workflows. However, health organizations are concerned that tightening the IT infrastructure through hardware and software security measures to safeguard patient data can hamper EHR interoperability. Therefore, in this study we investigate if the tightening of security measures to protect patient data could potential lead to a higher interoperability problems in the hospital’s EHR systems. We consider three facets (i.e. technical, semantic and organizational) of EHR interoperability in our study. The key to an interoperable EHR system is adherence to a standardized IT infrastructure and close coordination and collaboration between various stakeholders including software vendors, providers and patients. Hence, we argue that hospitals with fewer interoperability problems would be more efficient and effective in recovering from system downtime as the result of security failures. We utilize data on data security features and interoperability in 1800 acute care hospitals across 30 countries to explore the relationships and test the hypothesis. In our econometric analysis we also control for hospital characteristics, IT investment, IT staff, EHR type, EHR features, and Health Information Exchange standards followed by the hospitals. In our preliminary analysis we find no evidence that extensive use of data security measures in a hospital would hinder the interoperability of the EHR systems. We also find that that hospitals with fewer technical interoperability problems can come back to normalcy sooner post a system outage. The research findings would ease concerns of the hospitals regarding the impact of data protection initiatives on EHR interoperability. The study also recommends health organization to attain excellency in EHR interoperability to reduce financial loss as the result of an EHR downtime.