Security Control Techniques: Cybersecurity & Medical Wearable Devices

Samuel Sambasivam
Samuel.Sambasivam@Woodbury.edu
Computer Science Data Analytics
Woodbury University
Burbank, CA 91504

Jeff Deal
Jeff@n6networks.com
N6Networks

Abstract

The Internet of things (IoT) has been a significant advancement in technology, advancing the modernization of repetitive tasks, streamlining data collection, and providing new ways to collect, interpret, and disseminate information. Numerous industries have benefited from advancements in IoT technology, including the healthcare industry. For example, medical IoT (MIoT) has deployed several devices, including internet-connected sleep apnea, blood pressure regulators, glucose monitoring, and mobile echocardiogram and heart rate monitors. The advancement in MoT devices has revolutionized medicine and the treatment of care. Both treatment facilities and patients perform a significant amount of care solutions from their homes, saving the patient time and money. However, the integration of technology to maintain potential life-sustaining functions within the patients comes with the challenge of ensuring that data integrity and patient safety are not compromised. This study leveraged a qualitative case study to understand the security controls and techniques cybersecurity professionals need to protect medical wearable devices. Participants were selected from a wide range of medical treatment facilities, including information system technicians, information system security officers, and chief information officers. The top three cybersecurity concerns identified by survey respondents are 1) IT professionals require a better understanding of how devices function – including criticality of health care task, authentication protocol, data transmission details, etc. 2) users/wearers lack a fundamental understanding of cybersecurity risks and available security functions/features 3) the cooperative role required by the device manufacturer, the medical treatment professional, IT professional, and users to properly secure MIoTs is not understood. Recommendations for cybersecurity professionals identify MIoT devices' standards based on identifying and prioritizing device function as a substantial factor for security risk assessments and ensuring devices deployed multi-factor authentication while maintaining a robust patching and security framework.

Keywords: Medical Wearable Devices, MIoT, IoT, Cybersecurity.

An updated manuscript may be found on the JISAR website; https://jisar.org