Healthcare Transformation with Informatics and Artificial Intelligence
J. Mantas et al. (Eds.)

doi:10.3233/SHTI230438

An Overview About Connected Medical Devices and Their Risks

Marlon Luca MACHAL[a,1]
[a] *Tampere University, Faculty of Medicine and Health Technology*

Abstract. Connected medical devices may send and receive orders from other devices or networks, such as the internet. A connected medical device is often equipped with wireless connection, allowing it to interface with other devices or computers. Connected medical devices are becoming more popular in healthcare settings because they provide a variety of advantages, such as quicker patient monitoring and more efficient healthcare delivery. Connected medical devices may help doctors make educated treatment decisions, enhance patient outcomes, and lower costs. The usage of connected medical devices is especially beneficial for patients who reside in rural or distant locations, have mobility limitations that make traveling to a healthcare center difficult, or during the COVID-19 epidemic. Monitoring devices, infusion pumps, implanted devices, autoinjectors, and diagnostic devices are among the connected medical devices. Smartwatches or fitness trackers that monitor heart rate and activity levels, blood glucose meters that can upload data to a patient's electronic medical record, and implanted devices that can be monitored remotely by healthcare practitioners are examples of connected medical devices too. Yet, connected medical devices also carry risks that might jeopardize patient privacy and the integrity of medical records.

Keywords. Connected Devices, Risk, Patients.

1. Introduction

A connected medical device is one that can connect to other devices or networks, such as the internet, to exchange, transfer, or receive commands from other devices or the device's user [1, 2, 3]. A connected medical device is often equipped with wireless connection, allowing it to interface with other devices or computers [4, 5]. Connected medical devices are becoming more popular in healthcare settings because they provide a variety of advantages, such as quicker patient monitoring and more efficient healthcare delivery [6]. Connected medical devices have the potential to improve healthcare delivery by offering real data and insights that assist healthcare professionals in making informed treatment choices, improving patient outcomes, and lowering costs [7]. Connected medical devices are also being utilized to enable telemedicine to monitor patients with chronic illnesses like diabetes or heart disease, allowing healthcare professionals to check their health state and intervene as needed [8]. The usage of

[1] Corresponding Author, Marlon Luca Machal, Tampere University, Faculty of Medicine and Health Technology, Arvo Ylpön katu 34, 33520 Tampere, Finland; E-mail: marlon.machal@tuni.fi.

connected medical devices is especially beneficial for patients who reside in rural or distant locations, have mobility limitations that make traveling to a healthcare center difficult, or during the COVID-19 epidemic. Monitoring devices, infusion pumps, implanted devices, autoinjectors, and diagnostic devices are among the connected medical devices. Smartwatches or fitness trackers that monitor heart rate and activity levels, blood glucose meters that can upload data to a patient's electronic medical record, and implanted devices that can be monitored remotely by healthcare practitioners are examples of connected medical devices too [9].

2. Methods

This paper is a systematic review of several literatures related to connected medical devices. The supporting material originated from the US FDA Manufacturer and User Facility Device Experience and recall records. The aim of this paper is to increase people's understanding of the risks posed by connected medical devices.

3. Risk associated with connected medical devices

While connected medical devices provide several potential benefits, they also pose a number of risks that must be carefully managed in order to maintain patients' safety and privacy. Cybersecurity concerns, data privacy, technical failure, interoperability, user error, and regulatory compliance are all well-known risks associated with connected medical devices [10, 11]. Cyberattacks on connected medical devices may jeopardize patient privacy and safety. Hackers may obtain access to patient data or take control of medical devices, putting patients at danger. Unauthorized access to sensitive patient data is one of the key cybersecurity risks in connected medical devices. Connected medical devices collect and send massive quantities of sensitive patient data, such as health records, test results, and prescription doses, which may be exploited by cybercriminals. Hackers might obtain a copy of this data, steal it, or modify it in order to harm patients. Another risk is the possibility of unauthorized access to the device's software, which might result in device failure or inappropriate medicine administration. Malware, such as viruses or ransomware, might infiltrate connected medical devices, causing software faults or device failure. This failure may lead to erroneous dosage, therapy delays, or other significant consequences. Poor or obsolete security measures may significantly raise the risk of cyberattacks on medical devices that are connected. Many devices were not created with cybersecurity in mind from the start, and as a result, they lack basic security protections. As a result, they may be more exposed to cyberattacks, which may have significant implications on patients health.

Another risk with connected medical devices is data privacy. These devices create a large quantity of personal health data, which must be properly handled in order to safeguard patient privacy. If this data is misused or comes into the wrong hands, the repercussions for patients might be severe [11, 12]. Technical failure is a typical problem that may occur in any connected medical devices which can have major ramifications for patient safety. A faulty insulin pump, for example, might give the incorrect dosage of insulin, possibly resulting in a life-threatening condition [13, 14]. The technological failure is also related to the interoperability of the connected medical devices with other devices or networks. With so many different types of connected medical devices on the

market, it may be difficult to verify that these devices can interact with one another as intended. This may result in data silos, preventing healthcare practitioners from obtaining an accurate picture of a patient's health state. Even if the connected medical devices are or will be free of cybersecurity and technical fault and can interact with one another, the data created, exchanged, and stored by these devices must be reliable. In an ideal world, connected medical devices would consistently and precisely operate to assure patient safety and enable therapeutic effectiveness. The device's interoperability or failure might be attributed to user error. To utilize connected medical devices and analyze the data they create, healthcare practitioners and patients must be effectively trained. If they are not adequately trained, they may misunderstand data or operate the device incorrectly, putting patients at danger.

Regulatory compliance risk is related to failing to comply with applicable regulation, standards and guidance. Adherence to applicable standards and guidelines regulating the safe and effective use of connected medical devices is often used to establish compliance. Compliance with regulations may be difficult and vary around the world, and failure to comply with applicable regulations can result in legal and financial penalties.

4. Connected medical device and the control of medicine dosage

As part of dosage control, numerous connected medical devices are equipped with software that regulates the amount of medication administered to a patient. Software may be used by healthcare professionals (doctor or nurse) and/or patients to enter dosage instructions. These instructions are then automatically sent to a dispensing medical device, which measures and administers the appropriate amount of medicine. Special software used in connected medical devices can be classified as a medical device under EU and US medical device regulations. The use of software to manage dose has been shown to introduce potential risks and weaknesses that might compromise the device's accuracy and safety. Programming errors, bugs, and cyberattacks may all lead to failures or wrong doses in software. Software error already forced several companies to perform a recall of their devices from the market [15, 16, 17]. If the failure risk results in permanent injury or death of patients, requiring medical device manufacturers to add mechanical control dosage is an obligation rather than a suggestion. Mechanical manual dose control is a way of managing the dosage of medication administered by a connected medical device, such as an infusion pump, that does not rely exclusively on software controls. The use of mechanical manual dosage control can offer an additional degree of safety and security for patients who utilize connected medical devices.

Not all connected medical devices can use mechanical manual dose control. Mechanical manual control can increase the size and weight of the connected medical devices, which can affect its usability, portability, production and maintenance costs. Therefore, manufacturers must carefully balance the pros and cons of mechanical manual dose control in connected medical devices to determine if it is suitable for their product.

5. Conclusion

Connected medical devices improve patient outcomes and treatment efficiency through the collection and analysis of the data. Cyberattacks are expected to increase as

connected medical devices become more integrated and networked. Cybercriminals may utilize the connected medical devices' inherited vulnerability to misuse patient data or harm patients. Healthcare professionals and patients may use these devices safely and effectively to improve patient outcomes by prioritizing cybersecurity, training, and monitoring.

References

[1] Woods, B., Coravos, A., & Corman, J. D. (2019). The case for a hippocratic oath for connected medical devices. *Journal of Medical Internet Research*, *21*(3), e12568.

[2] Singh, R. P., Javaid, M., Haleem, A., Vaishya, R., & Ali, S. (2020). Internet of Medical Things (IoMT) for orthopaedic in COVID-19 pandemic: Roles, challenges, and applications. *Journal of clinical orthopaedics and trauma*, *11*(4), 713-717.

[3] Loncar-Turukalo, T., Zdravevski, E., da Silva, J. M., Chouvarda, I., & Trajkovik, V. (2019). Literature on wearable technology for connected health: scoping review of research trends, advances, and barriers. *Journal of medical Internet research*, *21*(9), e14017.

[4] Kadhim, K. T., Alsahlany, A. M., Wadi, S. M., & Kadhum, H. T. (2020). An overview of patient's health status monitoring system based on internet of things (IoT). *Wireless Personal Communications*, *114*(3), 2235-2262.

[5] Adeniyi, E. A., Ogundokun, R. O., & Awotunde, J. B. (2021). IoMT-based wearable body sensors network healthcare monitoring system. *IoT in healthcare and ambient assisted living*, 103-121.

[6] Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems*, *78*, 659-676.

[7] Kalid, N., Zaidan, A. A., Zaidan, B. B., Salman, O. H., Hashim, M., & Muzammil, H. J. J. O. M. S. (2018). Based real time remote health monitoring systems: A review on patients prioritization and related" big data" using body sensors information and communication technology. *Journal of medical systems*, *42*, 1-30.

[8] Pramanik, P. K. D., Upadhyaya, B. K., Pal, S., & Pal, T. (2019). Internet of things, smart sensors, and pervasive systems: Enabling connected and pervasive healthcare. In *Healthcare data analytics and management* (pp. 1-58). Academic Press.

[9] Kotalczyk, A., Imberti, J. F., Lip, G. Y., & Wright, D. J. (2022). Telemedical Monitoring Based on Implantable Devices—the Evolution Beyond the CardioMEMS™ Technology. *Current heart failure reports*, *19*(1), 7-14.

[10] Schwartz, S., Ross, A., Carmody, S., Chase, P., Coley, S. C., Connolly, J.& Zuk, M. (2018). The evolving state of medical device cybersecurity. *Biomedical instrumentation & technology*, *52*(2), 103-111.

[11] Ray, A. (2021). Cybersecurity for connected medical devices. Academic Press.

[12] Yle. (2022). Probe of psychotherapy firm's data breach finds possible European, employee links. https://yle.fi/a/3-12543823 (accessed on 28.02.2023)

[13] FDA. (2020). MAUDE Adverse Event Report: Medtronic minimed medtronic 670g insulin pump automated insulin dosing device system, single hormonal control. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/detail.cfm?mdrfoi__id=10534902&pc=OZP (accessed on 20.01.2023)

[14] Sherr, J. L., Heinemann, L., Fleming, G. A., Bergenstal, R. M., Bruttomesso, D., Hanaire, H., and Evans, M. (2022). Automated insulin delivery: benefits, challenges, and recommendations. A Consensus Report of the Joint Diabetes Technology Working Group of the European Association for the Study of Diabetes and the American Diabetes Association. Diabetes Care, 45(12), 3058-3074.

[15] FDA. (2021). BD to Begin Remediation for BD Alaris™ System Software. https://www.fda.gov/safety/recalls-market-withdrawals-safety-alerts/bd-begin-remediation-bd-alaristm-system-software#recall-announcement (accessed on 20.02.2023).

[16] FDA. (2020). Class 2 Device Recall t:slim X2 Insulin Pump with Dexcom G5 Mobile CGM and t:slim X2 Insulin Pump with BasaIIQ Technology. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfres/res.cfm?id=193503 (accessed on 20.02.2023).

[17] FDA. (2021). Class 1 Device Recall Baxter SIGMA Spectrum. Class 1 Device Recall Baxter SIGMA Spectrum (fda.gov) (accessed on 20.02.2023).