THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 4. Issue 3 (2024)
https://doi.org/ 10.62019/abbdm.v4i3.200

Security Risk Assessment of IoT for Remote Patient Monitoring System

Sumaira Memon, Lachhman D. Dhomeja, Shahzad A. Memon, Bisharat R. Memon, Nisar A. Memon, Khalid N. Charan

Chronicle

Article history

Received: june 22, 2024
Received in the revised format: July 3, 2024
Accepted: July 7, 2024
Available online: July 9, 2024

Sumaira Memon, Lachhman D. Dhomeja, Shahzad A. Memon, Bisharat R. Memon, Nisar A. Memon & Khalid N. Charan are currently affiliated with A.H.S Bukhari Institute of ICT, Faculty of Engineering & Technology, University of Sindh, Jamshoro, Pakistan.
Email: sumaira.memon@scholars.usindh.edu.pk
Email: lachhman@usindh.edu.pk
Email: shahzad.memon@usindh.edu.pk
Email: bisharat.memon@usindh.edu.pk
Email: nisar.memon@usindh.edu.pk
Email: khalid.charan@scholars.usindh.edu.pk

Corresponding Author*

Abstract

Remote Patient Monitoring (RPM), an essential component of telehealth, is among the biggest changes marked in healthcare. It facilitates patients' treatment, remotely at home or in some distant location, without traditional clinical settings. The RPM plays a key role in data acquisition, data analysis and insights, and improved healthcare management. It collects real-time data using wearable sensors and mobile apps, and furnish crucial health metrics. Advanced algorithms and prognostic modelling than process the data, pattern and likely health risks to predict any disease more precisely and accurately for early action. RPM provides real-time watch and remote consultation that help in improved disease control and better patients' care. Improved accuracy, reduced cost, real time interaction, and refined patient well-being are the significant healthcare benefits of RPM. Prognosis Health & Management (PHM) system is used for predicting the remaining useful life (RUL) of healthcare assets such as sensors, pacemakers, defibrillators and other medical equipment. The PHM leads to pre-emptive maintenance, lowers downtime, and tracks the life span of such healthcare equipment. The IoT enables PHM to monitor remote assets and gather instant data to foresee the RUL of such equipment. Providing the facilitations, PHM also creates potential vulnerabilities of exposure of device, network and data, and poses data security and privacy challenges. Therefore, strong security controls are required to keep patients' data confidential and safe from uneven approaches to technology and data breaches. This paper evaluates risk associated with RPM using OCTAVE ALLGERO, a risk assessment framework, to mitigate the data security concerns.

Keywords: Remote Patient Monitoring; Prognostic Health Management; Operationally Critical Threat, Asset, and Vulnerability Evaluation; Remaining Useful Life.

INTRODUCTION

Prognostics and health management (PHM), an enabling technology, maintaining the operations of engineering equipment, systems and structures efficiently, economically, safely, and reliably (Hu et al., 2022). In the healthcare system, the PHM predicts the RUL of PRM healthcare assets such as sensors, pacemakers, defibrillators and other medical equipment. The PHM leads to pre-emptive maintenance, lowers downtime and costs, and tracking the life span of the equipment. Its main use in healthcare is to monitor the RUL of pacemakers and defibrillators. RPM healthcare and medical devices are among the significant areas for PHM to provide its services using IoT. The IoT facilitates PHM by enabling remote asset tracking and instant data gathering, which makes the security of

these devices vital for trustworthy prognostic data (Ahmed et al., 2023). There exist many data safety and security problems like exposure of device, network and data, and the lack of authentication, authorization and encryption. The security concerns surrounding these crucial systems entrusted with sensitive patient data and influencing life-saving decisions demand immediate attention. Selection of tools with integrated protection, establishing strong security for network infrastructure, encrypting data at rest and in transit, implementing security best practices, following established security guidelines such as monitoring and auditing that may continuously monitor systems for security threats and vulnerabilities, and additional security considerations should be taken to reduce this risk for specific PHM applications. Organizations can mitigate the risks of cyber-attacks by implementing these solutions and tailoring them to specific PHM applications and can protect the integrity and reliability of their RPM data. As RPM provides various advantages, it also introduces new security concerns that need to be focused upon. Some of the issues that come under the limelight are data privacy, device and network security, data security, integrity, insider threats, physical security, and incident response(LLC, 2023). In this paper, we assess potential security threats, one by one, using the risk assessment framework OCTAVE to mitigate the data security and privacy risk of RPM, effectively.

LITERATURE REVIEW

The growing reliance on Internet of Things (IoT) devices in healthcare promises transformative benefits for remote patient care and medical monitoring. However, this interconnected landscape also introduces security vulnerabilities, threatening user privacy, data integrity, and even patient health itself (Shamsi et al., 2016). RPM is one of the major applications of prognosis health management that frequently uses IoT devices such as sensors like smartwatches, wristbands, and patches. RPM includes the sending and receiving of data to the central system by doctors for diagnosis, allowing the initial detection of health problems and predetermining mediation (Thomas et al., 2021).This helps in decreasing visits to health practitioners and allows customized care based on specific data patterns.

IoT-based systems are useful as long as their users remain safe. In IoT systems, all types of data collection and mining are performed over the Internet. Thus, personal data can be accessed at various stages (during collection, transmission and so on). Patients' safety should be taken into consideration by preventing any form of tracking or illegal identification. The higher the level of autonomy and intelligence of the IoT devices, the harder the protection of identities and privacy becomes. IoT based applications are also vulnerable because of wireless communication, which makes eavesdropping easier. Additionally, IoT devices generally have low energy and low computing power, which makes it harder to implement complex algorithms to guarantee security. Rigorous research is needed to ensure privacy, trust, and security throughout the health-care environment (Kelly et al., 2020). Keeping medical information private is a big deal for both doctors and patients. Sharing test results through new connected technology can be scary, because people worry that it might not be kept secret (Sonune et al., 2017). Hackers could be drawn to this technology, and experts warn it might not always be set up securely (Poyner & Sherratt, 2018). This worry grows when information is shared with many different apps. Weak security like passwords that nobody changes, or mistakes in

setting up the internet, could open the door for someone to see private medical details. Even where you buy medicine and where you go can give hints about your health, and that information might be shared too. Some doctors and hospitals have to give certain information to the police by law, which can worry patients even more and make them less likely to use the technology. The different ways information travels online, often managed by companies we don't know, makes it even harder to keep everything safe and private (Williams & McCauley, 2016). Medical and RPM devices capturing sensitive data are inherently vulnerable due to their connectivity through the "device layer," often the firmware responsible for communication (Vijayan et al., 2021). This exposes them to diverse attacks, such as:

(a) RPM breach. Unauthorized access to devices,

(B) Physical tampering with devices like Lifeline Hijack. Exploiting RPM Device Vulnerabilities,

(c) RPM firmware flaw. Exploitation of un-patched vulnerabilities in device firmware, there are various attacks at different layers of RPM.

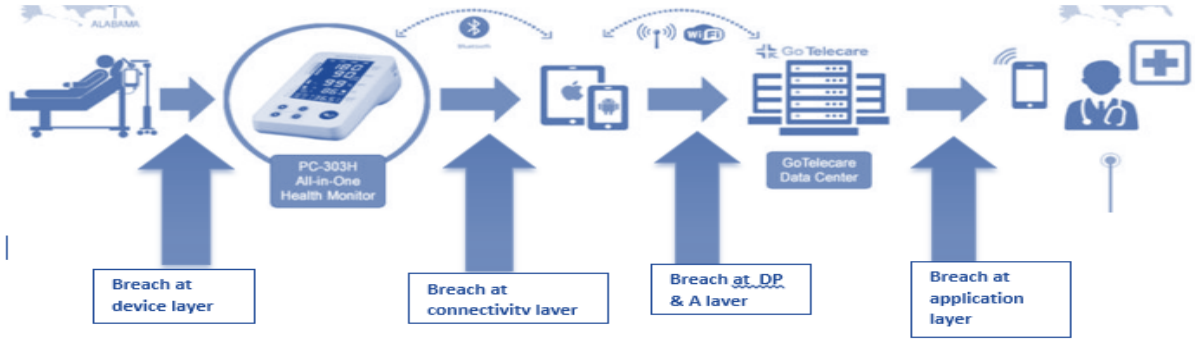

Figure 1.
source of breaches at different layers of RPM

Disclosing security threats in these devices remains a challenge, as shown in figure 1, due to several factors (Aziz et al., 2023):

(a) Complex vulnerabilities: The intricate nature of IoT systems offers a vast attack surface, increasing the risk of exploitation

(b) Expanded attack landscape: Internet connectivity exposes devices to a wider range of potential threats

(c) Inadequate security: Weak default authentication and unstable web access amplify vulnerabilities and make devices more susceptible to attack

(d) Lack of standards: The absence of robust and consistent security protocols allows attackers to exploit known vulnerabilities across different manufacturers and models.

RPM TECHNOLOGY

RPM works with healthcare data and IoT sensor devices like smart watches and wearables. It collects personal and very dedicated data such as vital signs, medication,

and diagnosis (Hariharan et al., 2021). Ensuring the safety of this data violation, exposure, and illegal access is crucial. Healthcare data is bound to follow strict regulations like HIPAA and GDPR, so it requires constancy to data security and privacy. Whereas normalizing the need for accurate health perception with patient anonymity and data privacy through unnamed and aggregation techniques is complex. The security of data at all stages of data transmission from the device to the cloud platform is significant to avoid interruption or loss of data (Hoffman, 2022). To maintain data security and prevent attacks, devices and software components must be updated.

These challenges necessitate immediate action in the form of:

(a) Enhanced device security: Robust security protocols, encryption, and secure authentication mechanisms

(b) Standardized security frameworks: An industry-wide standard for secure development, deployment, and maintenance

(c) Vulnerability transparency: Manufacturers must be encouraged to be transparent about vulnerabilities and issue prompt security updates

(d) Cybersecurity awareness: Educating healthcare professionals and users about threats and best practices is vital (Jawad, 2024).

By addressing these vulnerabilities and implementing effective security measures, we can utilize the potential of IoT in healthcare while safeguarding patient privacy, data integrity, and ultimately, patient safety. Some appropriate actions should be taken before these interconnected devices become gateways to harm rather than instruments of healing. In the context of IoT for PHM, several layers are involved in handling data (Tianshu et al., 2019). These layers are device layer, connectivity layer, data processing and analytical layer, application layer, and security and privacy layer. It is noteworthy that the efficiency of prognostic health management depends on the ability of the data processing and analytics layer. This layer determines historical data and performs real-time analysis to make decisions and take preventive actions. The intelligence derived from this layer contributes to overall health monitoring, diagnosis, and prognosis of the system (Li et al., 2024). The overall structure of RPM is shown in Figure 2.

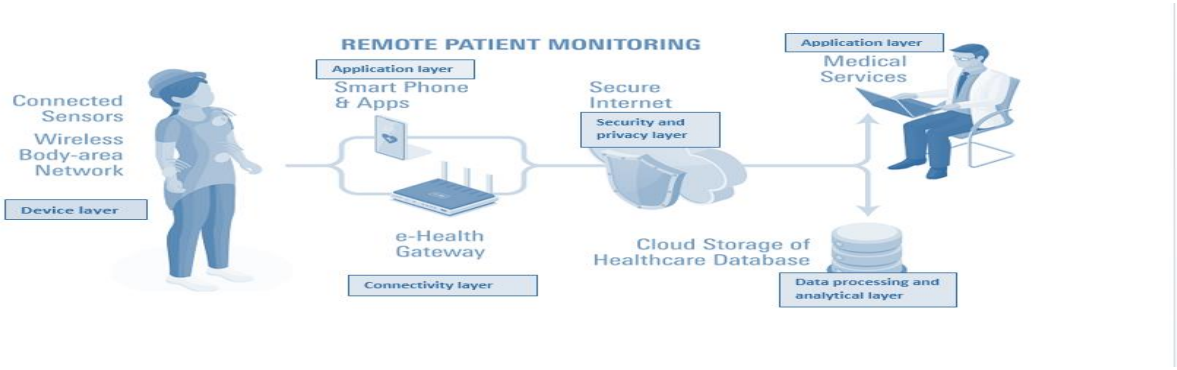

Figure 2.
Overall architecture of RPM

Device Layer: This layer operates at the physical aspect of IoT where sensors and actuators are present. It aids in the collection of raw data related to the health and

performance of monitored systems.

Connectivity Layer: This layer focuses on the transmission of data between devices and CPUs or cloud platforms. It serves as a bridge between the device layer and the data processing and analytics layer.

Data Processing and Analytics Layer: This is the core layer of prognostic health management, dealing with data. It processes raw data from IoT devices, transforming it into meaningful information. It uses analytics techniques such as machine learning and statistical analysis to identify patterns, anomalies, predict potential issues, and provide detailed and applicable information based on the processed data.

Application Layer: This layer relies on the data provided by the data processing and analytics layer. It integrates specific PHM application interfaces for end-users and summarizes the results into recommendations.

Security and Privacy Layer: This layer implements measures such as data encryption, access controls, and secure communication protocols to protect information.

RISK ASSESSMENT OF RPM

We use OCTAVE ALLGERO risk assessment framework for securing RPM layers as discussed in the previous section. OCTAVE can be highly suitable for assessing RPM systems. It facilitates the identification of critical assets, the analysis of threats and vulnerabilities, the prioritization of risks, and the implementation of appropriate controls (Gartner Researc, 2010). This structured approach helps optimize resource allocation, leading to an enhanced security posture. Additionally, OCTAVE promotes continuous improvement through iterative assessments and updates. While not a specific version of OCTAVE, ALLGERO is a complementary methodology that adds depth and detail to the risk assessment process. By considering operational context, countermeasure effectiveness, and cost-benefit analysis, ALLGERO can further guide decision-making and prioritize investments in security improvements. It consists of following six steps:

Step 1: System Characterization

IoT for RPM is one of the important aspects of prognostic health management application. It consists of six layers including Device layer, Connectivity layer, Data processing and analytical layer, Application layer, Security and privacy layer.

Step 2: Threat Identification

This step identifies threats to RPM systems. Threats can originate from digital attacks or physical damage to devices or hardware. They are categorized into two main categories: Insider threats: Initiated from within the organization, can be malicious (intentional harm) or unintentional (negligence, errors). Outsider threats: Originate from external actor, such as hackers, cybercriminals, or competitors. Aim to exploit vulnerabilities in systems or networks to gain unauthorized access. In this step, we have identified faults in software, weak configurations, and vulnerabilities in security. We have discussed potential threat actions that could exploit these vulnerabilities, potentially leading to specific threats within the RPM system. The following table outlines these threats according to their corresponding layers.

Table.1
Identification of threats for RPM

Threat	Motivation	Threat Action
	Insider	
Physician	Monetary Gain	Fraud and data theft
	Unintentional Error	Input of falsified data
Family Member		Sale of personal data
		Unauthorized system access
Outsider		
Attackers	Unauthorized Data Modification	Information theft
	Illegal information disclosure	Intrusion of privacy
	Destruction of information	System attacks e.g. denial of service
		System intrusion
		System tampering
		Unauthorized system access

Step 3: Identification of vulnerability

a. **Device Layer:** The device layer is responsible for data collection and has vulnerabilities such as a lack of authentication and authorization, insecure physical interfaces, and insufficient device firmware security. The threat sources may be outsiders or insiders, as shown in Table 2.

Table 2:
Vulnerabilities at device layer of RPM

Vulnerability Lack of Authentication and Authorization	Threat source Outside/insider	Threat action RPM breach: Unauthorized access to devices
Insecure Physical Interfaces	Outsider	Physical tampering with devices Lifeline Hijack: Exploiting RPM Device Vulnerabilities
Insufficient Device Firmware Security	Outsider	RPM firmware flaw: Exploitation of unpatched vulnerabilities in device firmware,

b. **Connectivity Layer:** The connectivity layer is responsible for transmission. It may have vulnerabilities such as inadequate encryption practices and weak network security. These vulnerabilities can be exploited by outsiders or insiders as shown in Table 3.

Table 3.
Vulnerabilities at connectivity layer of RPM

Vulnerability	Threat source	Threat Actions
Inadequate Encryption Practices	Outsider	Threat: Man-in-the-middle attacks, eavesdropping, and unauthorized access during data transmission between devices and central systems.
Weak Network Security	Outsider	RPM network breach: Unauthorized access to the network, potentially

c. Data Processing and Analytics: It is the core layer of PHM. It also has vulnerabilities such as insufficient data encryption and data integrity, as explained in Table 4, along with its threat sources and threat actions.

Table 4.
Vulnerabilities at data processing and analytics layer of RPM

Vulnerability	Threat source	Threat Action
Insufficient Data Encryption	Insider/outsider	Prognosis breach: Unauthorized access to processed health data
Data Integrity Risks	Insider/outsider	Data tampering: Tampering with processed data,

d. **Application layer:** In Table 5, vulnerabilities at the application layer, such as weak authentication in applications and insecure data storage, are explained along with their threat actions (what will happen to the system and data if these vulnerabilities are exploited?) and threat sources.

Table 5.
Vulnerabilities at application layer of RPM

Vulnerability	Threat source	Threat action
Weak Authentication in Applications	Outsider	Prognosis health breach: Unauthorized access to prognostic health applications,
Insecure Data Storage	Outsider/insider	Patient data exposed: Breaches in data storage security

e. **Security and Privacy layer:** The Security and Privacy Layer works with security controls. It has vulnerabilities like insufficient access control and privacy policy violations, as discussed in Table 6, along with threat sources and threat actions.

Table 6: Vulnerabilities at security and privacy layer of RPM

Vulnerability	Threat Source	Threat action
Insufficient Access Controls	Outsider	RPM config hijack: Unauthorized individuals gaining access to security configurations,
Privacy Policy Violations	Outsider	Privacy breach: Non-compliance with privacy regulations,

Step 4: determining Likelihood Level: In this step, the likelihood of RPM vulnerabilities has been calculated by considering the relationship between the threats and the sources. For example, the likelihood will be high if the threat source is highly motivated, it will be medium if the threat source is moderately motivated, and low if the threat source lacks motivation. This is also discussed below.

High	Threat-source is highly motivated and sufficiently capable
Medium	Threat-source is motivated and capable.
Low	Threat-source lack motivation or capability.

Step 5: Impact Analysis: This step explains the effect of vulnerabilities on the system and data, and calculates the impact by considering the level of damage caused by exploited vulnerabilities. For example, the impact may be considered high if the vulnerability affects both patient data and the system, medium if it only harms one component (either the patient or data), and low if the vulnerability does not affect either. This is also discussed below.

High	Vulnerability may harm both the Patient Data and system
Medium	Vulnerability may only harm to either Patient Data or System
Low	Vulnerability harm may not affect to system or patient data

Step 6: Risk Determination

For the likelihood levels, each is given a level of 1.0 for high, 0.5 for medium and 0.1 for low.

For the impact levels, each is given a level of 10 for high, 5 for medium and 1 for low.

For resulting matrix, 0.1 - 1 being low, 1 - 5 being medium and 6 - 10 being high

Results

In this section, we discuss the results calculated using the risk matrix presented in Table 7. These results were obtained by assessing the likelihood and impact values outlined in sections D and E.

Table 7.
Risk Matrix for assessing risk level of RPM

Threat Likelihood	**Impact**		
	Low	**Medium**	**High**
High	1.0*1	1.0*5	1.0*10
Medium	0.5*1	0.5*5	0.5*10
Low	0.1*1	0.1*5	0.1*10

a. **Device layer:** Table 8 shows the risk level of the RPM at device layer by multiplying the values of likelihood and impact for each vulnerability. Such as, lack of authentication and authorization and insufficient device firmware security have a medium likelihood and risk level and high impact, while insecure physical interfaces have a high likelihood, impact and risk level, and insufficient device firmware security has medium likelihood, impact and risk level.

Table 8.
Risk level at device layer of RPM

Vulnerability	Threat action	Likelihood	Impact	Risk	level
Lack of Authentication and Authorization	RPM breach: Unauthorized access to devices,	0.5	10	5	Medium
Insecure Physical Interfaces	Physical tampering with devices Lifeline Hijack: Exploiting RPM Device Vulnerabilities	1	10	10	High
Insufficient Device Firmware Security	RPM firmware flaw: Exploitation of unpatched vulnerabilities in device firmware,	0.5	5	2.5	Medium

b. **Connectivity layer:** Table 9 shows the risk levels for vulnerabilities at the connectivity layer. Here, inadequate

encryption practices have a high likelihood, impact and risk level, while weak network security has a medium impact and risk level and high likelihood.

Table 9.
Risk levels at connectivity layer of RPM

Vulnerability	Threat Action	Likelihood	Impact	Risk	Level
Inadequate Encryption Practices	Threat: Man-in-the-middle attacks, eavesdropping, and unauthorized access during data transmission between devices and central systems.	1	10	10	High
Weak Network Security	RPM network breach: Unauthorized access to the network, potentially	1	5	5	medium

c. **Data processing and analytical layer:** Table 10 shows results for vulnerabilities at the data processing and analytical layer, where both vulnerabilies, insufficient data encryption and data integrity carry a medium risk level, and low likelihood and medium impact.

Table 10.
Risk level at data processing and analytical layers of RPM

Vulnerability	Threat action	Likelihood	impact	Risk	Level
Insufficient Data Encryption	Prognosis breach: Unauthorized access to processed health data	1	5	5	medium
Data Integrity Risks	Data tampering: Tampering with processed data	1	5	5	medium

d. **Application layer:** Table 11 shows the risk levels of vulnerabilities at the application layer. Weak authentication in applications and insecure data storage have medium risk levels. it also has a low likelihood for both vulnerabilities and has medium impact.

Table 11.
Risk level at application layers of RPM

Vulnerability	**Threat action**	**Likelihood**	**Impact**	**Risk**	**Level**
Weak Authentication in Applications	Prognosis health breach: Unauthorized access to prognostic health applications,	1	5	5	Medium
Insecure Data Storage	Patient data exposed: Breaches in data storage security	1	5	5	medium

e. **Security and privacy layers:** It has a high likelihood, impact and risk level for insufficient access control vulnerability and medium likelihood, impact and risk level of privacy policy violation as shown in table 12.

Table 12.
Risk levels at security and privacy layer of RPM

Vulnerability	**Threat action**	**Likelihood**	**Impact**	**Risk**	**Level**
Insufficient Access Controls	RPM config hijack: Unauthorized individuals gaining access to security configurations,	1	10	10	High

Privacy Violations	Policy	Privacy breach: Non-compliance with privacy regulations,	0.5	5	2.5	medium

Mitigation for RMP

- Implement a layered security approach: This means that organizations may combine device security measures, network segmentation, data encryption, intrusion detection, and access control to develop a layered defense mechanism against attacks.

- Choose secure devices: When selecting IoT devices, prioritize security features and reliable firmware/software mechanisms.

- Regularly update software and firmware: Ensure that devices are regularly updated with security and privacy enhancements.

- Segment and secure the network: Divide the RPM network from other significant systems to control the impact of breaches and integrate security measures into healthcare data.

CONCLUSION

RPM comprises various Internet of Things (IoT) devices that transmit sensitive healthcare information. PHM systems are deployed to maintain efficient, economical, safe, and reliable operations of RPM devices. PHM predicts the RUL and any impending fault of healthcare assets. Exposure of critical RPM equipment to the outside world creates data privacy and security vulnerabilities and threats. The robust security mechanism is essential at every layer of the system to ensure patient data confidentiality and integrity. We applied the OCTAVE risk assessment framework to identify the critical threats and associated vulnerabilities across different layers of the RPM architecture. Our analysis revealed that data manipulation poses the most significant risk with high-level threats particularly on the device, connectivity, and security & privacy layers. These findings emphasize the need of strong encryption, secure device authentication, and comprehensive data privacy practices to mitigate these vulnerabilities effectively.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributor of research and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally to the creation of this work.
Conflicts of Interests: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Ahmed Hany Dalloul, Farshad Miramirkhani, & Kouhalvandi, L. (2023). A Review of Recent Innovations in Remote Health Monitoring. Micromachines, 14(12), 2157–2157. https://doi.org/10.3390/mi14122157

Aziz, M., Elmedany, W., & Sharif, M. S. (2023). Securing IoT devices against emerging security threats: Challenges and mitigation techniques. *Journal of Cyber Security Technology*, *7*(4), 1–25. https://doi.org/10.1080/23742917.2023.2228053

Gartner Research, "The OCTAVE Risk Assessment Methodologies," Assessment Methodologies, 2010. https://www.gartner.com/en/documents/1405794 (accessed Jul. 01, 2023).

Hariharan, U., Rajkumar, K., T. Akilan, & J. Jeyavel. (2021). Smart Wearable Devices for Remote Patient Monitoring in Healthcare 4.0. *Internet of Things*. https://doi.org/10.1007/978-3-030-63937-2_7

Hoffman, S. (2022). Privacy and security — Protecting patients' health information. *New England Journal of Medicine*, *387*(21). https://doi.org/10.1056/nejmp2201676

Hu, Y., Miao, X., Si, Y., Pan, E., & Zio, E. (2022). Prognostics and Health management: a Review from the Perspectives of design, Development and Decision. *Reliability Engineering & System Safety*, *217*, 108063. https://doi.org/10.1016/j.ress.2021.108063

Jawad, L. A. (2024). Security and Privacy in Digital Healthcare Systems: Challenges and Mitigation Strategies. *Abhigyan*, *42*(1), 23-31.

Kelly, J. T., Campbell, K. L., Gong, E., & Scuffham, P. (2020). The internet of things: Impact and implications for healthcare delivery. Journal of Medical Internet Research, 22(11), e20135. https://doi.org/10.2196/20135

Li, C., Li, S., Feng, Y., Konstantinos Gryllias, Gu, F., & Pecht, M. (2024). Small data challenges for intelligent prognostics and health management: a review. *Artificial Intelligence Review*, *57*(8). https://doi.org/10.1007/s10462-024-10820-4

LLC, A. T. (2023, April 12). Addressing the Challenges of Remote Patient Monitoring: Security, Privacy, and Ethical Considerations. Accuhealth Technologies LLC. https://www.accuhealth.tech/blog/addressing-the-challenges-of-remote-patient-monitoring-security-privacy-and-ethical-considerations

Poyner, I. K., & Sherratt, R. S. (2018, March). Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people. In *Living in the Internet of Things: Cybersecurity of the IoT-2018* (pp. 1-5). IET.

Shamsi, J. A., Zeadally, S., Sheikh, F., & Flowers, A. (2016). Attribution in cyberspace: techniques and legal implications. Security and Communication Networks, 9(15), 2886-2900.

Sonune, S., Kalbande, D., Yeole, A., & Oak, S. (2017, June). Issues in IoT healthcare platforms: A critical study and review. In 2017 International Conference on Intelligent Computing and Control (I2C2) (pp. 1-5). IEEE.

Thomas, E. E., Taylor, M. L., Banbury, A., Snoswell, C. L., Haydon, H. M., Gallegos Rejas, V. M., Smith, A. C., & Caffery, L. J. (2021). Factors influencing the effectiveness of remote patient monitoring interventions: a realist review. *BMJ Open*, *11*(8). https://doi.org/10.1136/bmjopen-2021-051844

Tianshu, W., Shuyu, C., Jie, Y., & Peng, W. (2019, November). Intelligent prognostic and health management based on IOT cloud platform. In *2019 14th IEEE International Conference on Electronic Measurement & Instruments (ICEMI)* (pp. 1089-1096). IEEE.

Vijayan, V., Connolly, J. P., Condell, J., McKelvey, N., & Gardiner, P. (2021). Review of wearable devices and data collection considerations for connected health. Sensors, 21(16), 5589.

Williams, P. A., & McCauley, V. (2016, December). Always connected: The security challenges of the healthcare Internet of Things. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)* (pp. 30-35). IEEE.