Journal of Information Technology and Integrity

Cybersecurity Benefits and Challenges of Advanced Healthcare Technologies

Cheryl Ann Alexander[1]*, and Lidong Wang[2]

[1]*Institute for IT Innovation and Smart Health, Mississippi, United States.*

[2]*Institute for Systems Engineering Research, Mississippi State University, Mississippi, United States.*

Article Details

Article Type: Research Article
Received date: 26th December, 2024
Accepted date: 17th January, 2025
Published date: 20th January, 2025

***Corresponding Author:** Cheryl Ann Alexander, Institute for IT Innovation and Smart Health, Mississippi, United States.

Citation: Alexander, C. A., & Wang, L., (2025). Cybersecurity Benefits and Challenges of Advanced Healthcare Technologies. *J Inform Techn Int, 3*(1): 104. doi: https://doi.org/10.33790/jiti1100104

Abstract

Advanced technologies, especially cutting-edge technologies have been increasingly used in healthcare because they can bring many benefits and thus enhance competitiveness in medical services and healthcare delivery. However, there are vulnerabilities, cyber risks, and cybersecurity challenges while utilizing these technologies. This paper deals with major advanced technologies in healthcare, including their benefits and the dangers in cybersecurity due to their use. The technologies include cloud, blockchain, telemedicine, and telehealth; Internet of Things (IoT), Internet of Medical Things (IoMT), Internet of Health Things (IoHT), mobile health (*m*-Health), wearables; 3D printing/additive manufacturing, big data/big data analytics; artificial intelligence (AI)/machine learning (ML)/deep learning (DL), and robotics. Data security, privacy, and ownership are major challenges when advanced technologies are used in healthcare.

Keywords: Cybersecurity, Cloud, Blockchain, Telemedicine, Internet of Medical Things (IoMT), Mobile Health (m-Health), 3D Printing, Big Data, Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), Robotics, Healthcare

Introduction

Five main areas comprise third-party risk management (TPRM): reputation risk, compliance risk, transaction risk, operational risk, and information security risk. NIST (National Institute of Standards and Technology) and ISO (International Organization for Standardization) frameworks can be used to design and run TPRM programs. Four classes of data have been described in an organization, and they include 1) public, 2) internal, 3) sensitive, and 4) restricted [1]. Data backup, recovery, and disaster recovery have been more significant and complicated than before. The recovery time (RTO) and the recovery point objective (RPO) are important metrics in a data protection plan. The RPO is how much data is agreed to be lost when a disaster occurs. The public cloud offers two major kinds of storage for backups: object storage and block storage (commonly presented as a filesystem). The operating systems of backup servers are the front door to the backup data. They must be the most up-to-date and secure [2].

Managing risk is a complicated and multifaceted activity. Security, privacy, and supply chain risk management are not static. Security and privacy programs require close collaboration. A three-level approach is utilized to address the risk management process in an organization, which is shown in Figure 1 [3].

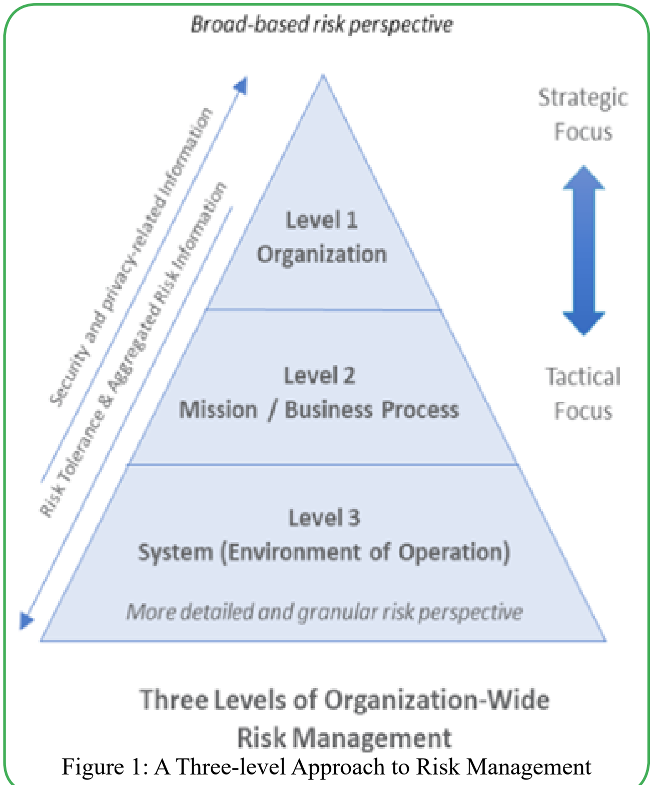

Broad-based risk perspective
Security and privacy-related information
Risk Tolerance & Aggregated Risk Information
Strategic Focus
Level 1
Organization
Level 2
Mission / Business Process
Tactical Focus
Level 3
System (Environment of Operation)
More detailed and granular risk perspective
Three Levels of Organization-Wide Risk Management

Figure 1: A Three-level Approach to Risk Management

Healthcare data sources include multiple sources, including patients, imaging data, diagnostic data, billing and other financial data, demographic data, and caregivers' notes. Data in healthcare-related processes include a variety of source-related data. Diagnostic data include laboratory, imaging, and physical assessments by caregivers. Data from medical providers contributes to related processes in planning and evaluation. Privacy is essential to healthcare data collection and should always be protected. The federal government has determined that protecting patient data should be a priority for all healthcare entities. Therefore, HIPAA and HiTech were constructed as a standard of data protection for all healthcare entities and include all healthcare data.

Emerald Healthcare System is a not-for-profit corporation dedicated to developing medical programs, healthcare services, research, etc. The system's three hospital campuses, plus several outpatient facilities, offer a broad spectrum of care. Services provided by over 1,550 medical staff members and more than 10,300 employed professionals, make Emerald Healthcare System one of the largest healthcare providers in Texas, USA. Advanced technologies have been used in the Emerald Healthcare System. There are vulnerabilities, cyber risks, and cybersecurity challenges in the healthcare system and providers while they benefit from advanced technologies.

The primary reason for the research in this paper lies in a discussion about major advanced healthcare technologies. The research methodology in this paper is literature research on major advanced healthcare technologies, plus benefits and challenges/risks in cybersecurity and their use in the Emerald Healthcare System in Texas, USA. Literature research was conducted using the database EBSCO via 'Advanced Search' to search papers on "cloud" and "cybersecurity", "blockchain" and "cybersecurity", "telemedicine" and "cybersecurity", "telehealth" and "cybersecurity", "Internet of Things" and "cybersecurity", "Internet of Medical Things" and "cybersecurity", "Internet of Health Things" and "cybersecurity", "Mobile Health" and "cybersecurity", "Wearables" and "cybersecurity", "3D printing" and "cybersecurity", "additive manufacturing" and "cybersecurity", "big data" and "cybersecurity", "big data analytics", "artificial intelligence" and "cybersecurity", "machine learning" and "cybersecurity", "deep learning" and "cybersecurity", and "robotics" and "cybersecurity". 'Subject Terms' was selected as 'Field' in the EBSCO database for searching papers. Targeted papers were published between January 2013 and October 2024 in English and scholarly (peer-reviewed) journals or conferences. Duplicated papers and weak papers were removed. The number of quality papers selected for the literature review is 106, but only 20 papers were cited in this paper because the papers matched the topics and the research objectives of this paper.

The remainder of this paper will be organized as follows: the second section introduces cloud and blockchain; the third section presents telemedicine and telehealth; the fourth section introduces IoT, IoMT, IoHT, m-Health, and wearables; the fifth section presents 3D printing/additive manufacturing and big data/big data analytics; the sixth section introduces AI/ML/DL and robotics; and the seventh section is the conclusion.

Cloud and Blockchain

Cloud can store and manage much healthcare data across various healthcare providers. This facilitates storing and sharing healthcare data. Cloud security is an important issue. There has been much research on data security in the cloud. The solutions to cloud security include encryption, multi-factor authentication (MFA), etc. [4].

Blockchain enables a secure and transparent approach to storing and transferring healthcare data. Blockchain security improves data privacy, identity management, and supply chain management. A great increase can be anticipated in the application of blockchain in cybersecurity. Blockchain security includes utilizing smart contracts, secure multi-party computation, and zero-knowledge proofs to guarantee data security and privacy [4].

Telemedicine and Telehealth

Telemedicine and telehealth have been transformative forces in healthcare. They provide patients with novel solutions for enhancing convenience, access, and healthcare quality. Providers have significantly improved healthcare delivery through telemedicine and other unique services. However, improved healthcare delivery also brings up challenges, vulnerabilities, and risks. Data security and privacy are critical areas of cybersecurity concerns. The platforms of telemedicine and telehealth handle sensitive patient data (such as personal information and medical records). It is significant to ensure the security and privacy of patient data. MFA is commonly recommended to reinforce user verification. Healthcare providers should practice robust cybersecurity by implementing strong authentication protocols, encrypting patient data, and providing frequent software updates to protect against vulnerabilities [5].

IoT, IoMT, IoHT, *m*-Health, and Wearables

Healthcare has changed greatly due to the emergence of IoT branches such as IoMT. IoMT helps reduce unnecessary hospital visits by linking patients to doctors. However, the security of IoMT devices is a major concern. Healthcare data in an IoMT system should be protected at all phases, including data capture, gathering, transmission, and archiving. A comprehensive evaluation of all available security methods and possible cyber threats is necessary for a robust cybersecurity program [6].

IoHT is characterized by interconnected medical devices that share sensitive patient data, which increases cyber risks and threats. It is critical to ensure the following: integrity, confidentiality, and availability of healthcare data. A hybrid deep learning-based intrusion detection system was proposed to tackle cybersecurity threats in IoHT [7].

Mobile health (*m*-health) refers to mobile telecommunications technologies that improve health by providing multiple ways to provide healthcare through the Internet. It can be an appropriate solution to improving the quality of nursing care, enabling remote visits, and reducing healthcare costs; therefore, promoting the elderly's empowerment, improving monitoring, preventing chronic diseases, and supporting healthcare at home. Data security, privacy, and ownership are major challenges [8].

Wearable devices have made patient monitoring and the comprehension of daily behaviors straightforward. Wearable devices have been employed in healthcare to monitor patients' health conditions and obtain body information. Wearables have the potential to increase access to timely care and treatment. IoT-based wearables, such as smartwatches, sensors, wearable biosensors, and wearable ECG monitors for healthcare monitoring are typically well-understood by most individuals However, data from sensors and wearables should be secure and safe by utilizing blockchain technology [9].

3D Printing/Additive Manufacturing and Big Data/ Big Data Analytics

3D printing or additive manufacturing has been used in healthcare, including patient-specific implants, prosthetics, dental products, bespoke instruments, customized pharmaceuticals, etc. [10]. It helps manufacture complicated tablet geometries, improving their solubility and bioavailability [11]. However, it is subject to regulations. The effects of their local legal implementation associated with 3D printing cannot be fully overseen [12].

The complexity of healthcare data is usually revealed in genomic data, population data, radiology images, clinical trial data submissions, financial or operational data, etc. Healthcare systems generate big data. Big data analytics handles healthcare big data [13]. Data security, privacy, data ownership, data governance, etc. are some challenges of big data in healthcare [14]. Hacking and other unauthorized access are common security problems.

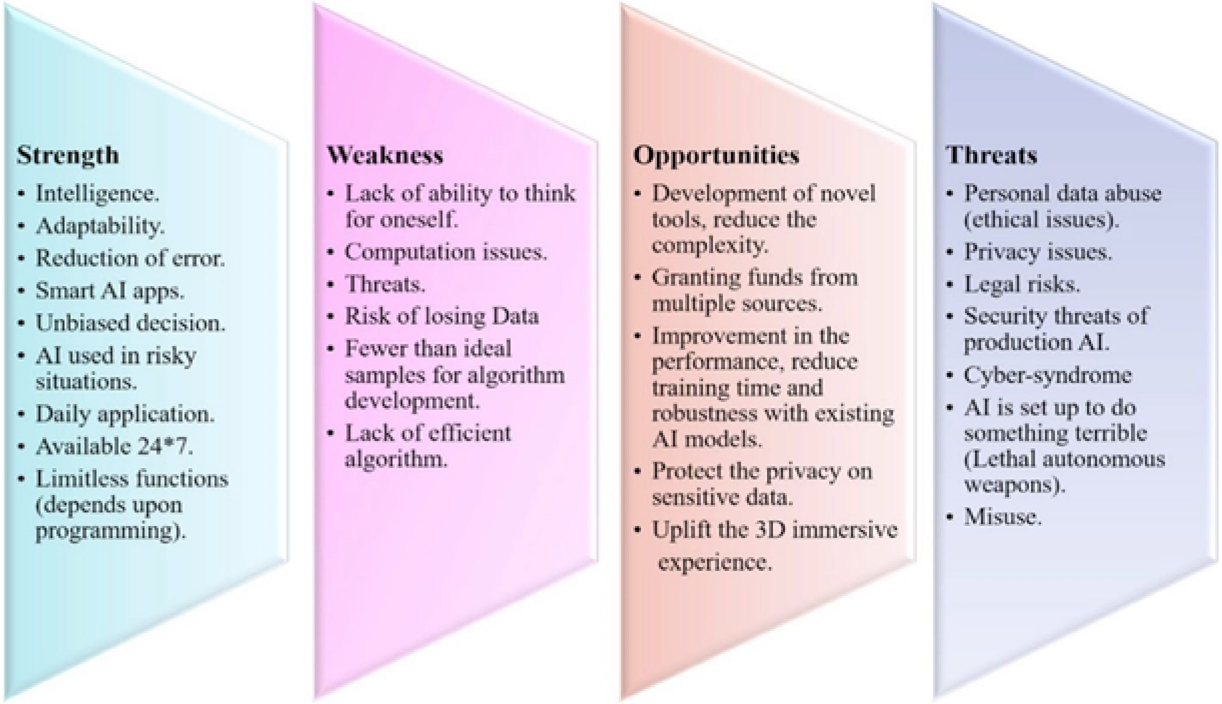
AI/ML/DL, and Robotics

ML and Robotics are sub-areas of AI. DL is one of the methods in ML. AI can be used in healthcare as follows [15]:

- Monitor patients' health information, such as heart rate and blood pressure, and notify healthcare professionals if anything is abnormal.

- Analyze medical images such as X-rays and MRIs to recognize disorders.
- Provide patients with information and support.
- Help create new medications.

A SWOT analysis of AI is shown in Figure 2 [15]. The SWOT analysis helps the development of AI in healthcare systems.



Strength

- Intelligence.
- Adaptability.
- Reduction of error.
- Smart AI apps.
- Unbiased decision.
- AI used in risky situations.
- Daily application.
- Available 24*7.
- Limitless functions (depends upon programming).

Weakness

- Lack of ability to think for oneself.
- Computation issues.
- Threats.
- Risk of losing Data
- Fewer than ideal samples for algorithm development.
- Lack of efficient algorithm.

Opportunities

- Development of novel tools, reduce the complexity.
- Granting funds from multiple sources.
- Improvement in the performance, reduce training time and robustness with existing AI models.
- Protect the privacy on sensitive data.
- Uplift the 3D immersive experience.

Threats

- Personal data abuse (ethical issues).
- Privacy issues.
- Legal risks.
- Security threats of production AI.
- Cyber-syndrome
- AI is set up to do something terrible (Lethal autonomous weapons).
- Misuse.

Figure 2: A SWOT Analysis of AI

A healthcare system with autonomous AI was studied. Cybersecurity autonomous AI can be practiced for 1) self-optimizing predictive cyber risk analytics of failures in a healthcare system during a Disease X event (undefined future pandemic), 2) self-adaptive forecasting of medical production and supply chain bottlenecks during future pandemics [16]. ML has been used in healthcare, cybersecurity, and other fields. Quantum computing (QC) helps ML to achieve the best performance and robust cybersecurity. ML and QC can be utilized by defenders and attackers/threat actors (cybercriminals). The benefits and challenges of cybersecurity are shown in Table 1 [17].

Methods	ML	QC
Defenders	• Analyze collected data to manage vulnerabilities and threat notifications. • Detect potential risks/attacks. • Fight security vulnerabilities/ weaknesses.	• Create accurate encryption codes quickly. • Detect threats/attacks fast.
Attackers/Threat actors	• Cybercriminals can also utilize it to create critical cyberattacks.	• Cybercriminals can also utilize it to break encrypted crypto codes fast.

Table 1: ML and QC benefits and challenges of cybersecurity

ML simplifies and appropriately diagnoses illnesses. Predictive analysis using ML helps perform accurate illness prediction and treatment. The application of ML to an intrusion detection system (IDS) is vital for dealing with rapidly evolving cyber-attacks [6]. IoT presents great potential in healthcare. The performance of deep learning models was evaluated for classifying cyber-attacks in IoT networks [18].

AI and robotics have been widely used in the pharmaceutical and medical sectors, as shown in Table 1 [11]. Cloud-integrated robotics or cloud robotics transforms rehabilitation and healthcare for people with disabilities. It empowers personalized and data-driven interventions. Table 3 [19] lists its applications, benefits, challenges, and the mitigations of the challenges.

Cybersecurity is a concern for robotic surgery. There is an inherent vulnerability in a complicated digital system. Surgical robots can be complicated; however, they are known to have points of vulnerability, and successful cyberattacks on surgical robots have occurred. Vulnerabilities were detected in robots that were used to deliver medical supplies in a hospital. There are approaches to improving the risk profile of robotic surgery, including recognizing system complexity, investing in regular software updates, following the best practices of cybersecurity, and improving transparency for all stakeholders [20].

Conclusion

The cloud can store and manage much healthcare data. The solutions to cloud security include encryption, MFA, and security orchestration of cloud environments. Blockchain enables a secure and transparent approach to storing and transferring healthcare data. Telemedicine and telehealth have improved healthcare delivery greatly. Strong authentication protocols, encryption of patient data, and frequent software updates help protect against vulnerabilities.

Aspects	Details
Drug discovery & healthcare	• Drug discovery (compound screening, de novo drug design, drug repurposing, biomarker discovery, etc.) • Predictive analytics • Early disease detection • Diagnostics and imaging • Precision medicine • Virtual health assistants • Etc.
Pharmaceutical manufacturing	• Automation of manufacturing processes • Automated mixing and dosing systems • High-speed sorting and analysis • Collaborative robots in drug manufacturing • 3D printing of drugs • Robotic quality control systems • Packaging and labeling • Warehousing operations
Drug delivery systems	• Robotic pharmacy dispensing systems • Implantable drug delivery devices • Nanorobotic drug delivery • Wearable drug delivery systems • Robotic exoskeletons for drug delivery • Etc.
Technologies in medicine	• Diagnostic robots • Robotic surgery • Rehabilitation robotics • Telemedicine robots • Laboratory automation • Etc.
Challenges & ethical considerations	• Data security & privacy • Accountability & liability • Accessibility & Affordability • Bias & fairness • Informed consent • Human interaction • Regulatory oversight • Etc.

Table 2: AI and robotics in the pharmaceutical and medical sectors

Aspects	Description
Applications	• Robotic exoskeletons (with enhanced mobility, balance, and support) • Cloud-connected prosthetics • Communication devices (cloud-connected speech-generating devices for people with communication and speech problems) • Smart mobility aids (wheelchairs & mobility devices) • Home automation & assistance (controlling smart home devices)
Benefits	• Remote customization (considering users' needs & preferences) • Data analytics (in real-time) • Adaptive learning & assistance (learning from user interactions & adapting to varying conditions) • Improved collaboration (among caregivers, users, & healthcare professionals) • Enhanced accessibility (access to information, support, & services)
Challenges/ mitigations	• Data security & privacy/Secure data storage & robust encryption (mitigation) • Ethical & societal implications/Addressing ethical concerns about data ownership, consent, & potential job displacement • Latency and connectivity/Low-latency communication between cloud & assistive devices • Accessibility/Being accessible to diverse user groups • User training and acceptance/Guaranteeing users can employ cloud-connected assistive technologies effectively

Table 3: Cloud robotics: applications, benefits, challenges and mitigations

IoMT helps reduce unnecessary hospital visits. Healthcare data in an IoMT system should be protected at all phases. m-health improves the quality of nursing care, enables remote visits, and reduces healthcare costs. Data security, privacy, and ownership are major challenges. Wearables enhance access to timely care. The data from sensors and wearables should be secure and safe by utilizing blockchain.

3D printing has been used in healthcare. Healthcare systems generate big data. Big data analytics can be used to handle the data. Data security and privacy, data ownership, data governance, etc. are major concerns. AI/ML/DL has been used in healthcare. AI and robotics have been widely used in the pharmaceutical and medical sectors. Cloud robotics transforms rehabilitation and healthcare for people with disabilities.

Acknowledgments

The authors would like to express thanks to Technology and Healthcare Solutions, USA for its help and support.

Declaration of the use of AI tools

The authors declare that they did not use AI tools in writing this paper.

Conflict of interest

The authors would like to announce that there is no conflict of interest.

Ethics

In this article, ethical principles related to scientific research articles are observed. The corresponding author confirms that both authors have read, revised, and approved the paper.

References

1. Rasner, G. C., (2021). Cybersecurity and third-party risk: Third party threat hunting. John Wiley & Sons.
2. Preston, W. C., (2021). Modern Data Protection. " O'Reilly Media, Inc.".
3. National Institute of Standards and Technology. (2021). RMF for systems and organizations introductory course. NIST.
4. Radanliev, P., (2024). Integrated cybersecurity for metaverse systems operating with artificial intelligence, blockchains, and cloud computing. *Frontiers in Blockchain, 7*, 1359130.
5. Wright, J., & Burrell, D. N. (2023). Telemedicine Cybersecurity Protection in Reproductive Healthcare. *HOLISTICA–Journal of Business and Public Administration, 14*(2), 1-14.
6. Arora, P., Kaur, B., & Teixeira, M. A. (2021). Cybersecurity in IIoT and IoMT networks using machine learning algorithms—A survey. *ICTACT Journal on Communication Technology, 12*(4).
7. Algethami, S. A., & Alshamrani, S. S. (2024). A Deep Learning-Based Framework for Strengthening Cybersecurity in Internet of Health Things (IoHT) Environments. *Applied Sciences, 14*(11), 4729.
8. Pahlevanynejad, S., Niakan Kalhori, S. R., Katigari, M. R., & Eshpala, R. H. (2023). Personalized mobile health for elderly home care: a systematic review of benefits and challenges. *International Journal of Telemedicine and Applications, 2023*(1), 5390712.
9. Sam, M. F. M., Ismail, A. F. M. F., Bakar, K. A., Ahamat, A., & Qureshi, M. I. (2022). The effectiveness of IoT based wearable devices and potential cybersecurity risks: A systematic literature review from the last decade. *International journal of online and biomedical engineering, 18*(9), 56-73.
10. Jewell, C. M., & Stones, J. A. (2024). Rise of the (3D printing) machines in healthcare. *International Journal of Pharmaceutics*, 124462.
11. Stasevych, M., & Zvarych, V. (2023). Innovative robotic technologies and artificial intelligence in pharmacy and medicine: paving the way for the future of health care—a review. *Big Data and Cognitive Computing, 7*(3), 147.
12. Capek, L., & Schwarz, D. (2024). 3D printing traceability in healthcare using 3Diamond software. *Heliyon, 10*(12).
13. Chrimes, D., & Zamani, H. (2017). Using distributed data over HBase in big data analytics platform for clinical services. *Computational and mathematical methods in medicine, 2017*(1), 6120820.
14. Nunan, D., & Di Domenico, M. (2013). Market research and the ethics of big data. *International journal of market research, 55*(4), 505-520.
15. Sharma, N., & Jindal, N. (2024). Emerging artificial intelligence applications: metaverse, IoT, cybersecurity, healthcare-an overview. *Multimedia Tools and Applications, 83*(19), 57317-57345.
16. Radanliev, P., & De Roure, D. (2022). Advancing the cybersecurity of the healthcare system with self-optimising and self-adaptative artificial intelligence (part 2). *Health and Technology, 12*(5), 923-929.
17. Said, D. (2023). Quantum computing and machine learning for cybersecurity: Distributed denial of service (DDoS) attack detection on smart micro-grid. *Energies, 16*(8), 3572.
18. Becerra-Suarez, F. L., Tuesta-Monteza, V. A., Mejia-Cabrera, H. I., & Arcila-Diaz, J. (2024, May). Performance Evaluation of Deep Learning Models for Classifying Cybersecurity Attacks in IoT Networks. *In Informatics* (Vol. 11, No. 2, p. 32). MDPI.
19. Zhang, R., Zhou, Y., Zhang, J., & Zhao, J. (2024). Cloud-integrated robotics: transforming healthcare and rehabilitation for individuals with disabilities. *Proceedings of the Indian National Science Academy*, 1-12.
20. Gordon, W. J., Ikoma, N., Lyu, H., Jackson, G. P., & Landman, A., (2022). Protecting procedural care—cybersecurity considerations for robotic surgery. *npj Digital Medicine, 5*(1), 148.