Internet of Things (IoT): Cybersecurity Risks in Healthcare

Ruhi Patel
Old Dominion University

Internet of Things (IoT): Cybersecurity Risks in Healthcare

Ruhi Patel

COVA CCI Undergraduate Research

Fall 2020

December 9, 2020

Internet of Things (IoT): Cybersecurity Risks in Healthcare

The rapid growth and investment in the Internet of Things (IoT) has significantly impacted how individuals and industries operate. The Internet of Things (IoT) refers to a network of physical, technology-embedded objects that communicate, detect, and interact with their external environment or internal state (Hung, 2017). According to Tankovska (2020), IoT devices are estimated to reach 21.5 billion units by 2025. This technological boom is leading various industrial sectors to notice a quick increase in cybersecurity risks and threats. One industrial sector has been particularly vulnerable to numerous cyber threats across the globe: healthcare. Oliver Noble (2020), a data encryption specialist at *NordLocker*, suggests that cybercriminals target healthcare institutions because they store an overwhelming amount of patient information that is private, personal, and unchangeable. Healthcare organizations have a difficult time securing their cybersecurity infrastructure and the reasons for this will be further discussed in this paper.

According to leaders from the Deloitte Center for Health Solutions, healthcare has experienced the emergence of the Internet of Medical Things (IoMT), a connected infrastructure of medical technology, systems, and services that can collect, transmit, and analyze data, which is estimated to generate $158.1 billion in 2022 (Haughey et al., 2018). IoT in healthcare offers a variety of benefits that focus on patients, such as the ability to monitor patients' health more closely which allows health professionals to make timely decisions (Sciforce, 2019). Cybersecurity should be front and center regarding these IoT devices' architecture, especially in healthcare where reliance on IoT technology can easily turn into scenarios between life and death.

This paper will address cybersecurity problems related to IoT in healthcare, including why medical technology remains outdated, data privacy concerns, the effects of COVID-19, and vulnerabilities in medical IoT devices. Then, a variety of solutions will be examined to mitigate these cyber risks, such as implementing risk management, network segmentation, and legislative standards, laws, and regulations related to healthcare IoT.

The Problem

Within various healthcare facilities, such as hospitals, clinics, and research laboratories, there are numerous connected, yet insecure devices being used daily, both by patients and healthcare facilities (Hill, 2020). Arampatzis (2019) notes that many of these IoT devices and systems remain outdated and unpatched, or still use legacy operating systems with few cybersecurity controls. As a result, the healthcare industry continues to suffer from various cyber attacks, such as ransomware, data breaches, and Distributed Denial-of-Service (DDoS) attacks, all of which can disturb patient care, health delivery services, and medical treatments. To further complicate things, the 2019 coronavirus (COVID-19) pandemic has only escalated the vulnerabilities found in healthcare, especially with a renowned emphasis on telehealth services. The shift to remote healthcare now suggests that the medical devices a patient uses in their home are connected to their home network, thus increasing the risk of attackers intercepting the data in transit between the at-home patient’s device and a medical facility. Data privacy is also a valid concern in healthcare. Cyber professionals are seeing security issues resulting from unencrypted data in IoT hardware and software architecture that can allow cybercriminals to efficiently steal personable identifiable information (PII) and personal health information (PHI). Organizations that do not take the necessary steps to protect patient information violate privacy regulations, such as those outlined in HIPAA.

Medical Technology Remains Outdated and Unpatched

One of the main issues in healthcare is the continued presence and use of outdated and unpatched technological infrastructure, including the Internet of Things. Steve Morgan (2019), the editor-in-chief of *Cybercrime Magazine,* asserts that the mixture of outdated systems, lack of experienced cyber personnel, and highly valuable data all contributes to why healthcare is one of the most vulnerable industries for cyber attacks.

According to Bob Renner, CEO of cloud-based data management firm Liaison Technologies, IT infrastructure in any industry needs to be replaced every 10 years, but the healthcare industry in particular has already missed two of these technology change cycles, resulting in the loss of 20 years of advanced technology (as cited in Donovan, n.d.). As healthcare settings have already gone so long without updating their devices, it is even more of a challenge to currently replace every legacy system and get everything up to date. Revitalizing IT infrastructure would require significant amounts of resources, such as time, talent, and money, most of which might not be a hospital’s number one priority. Furthermore, when hospitals want to deploy new technology, they might run into trouble finding top talent that would be willing to make upgrades and handle older legacy infrastructure (Matthews, 2018).

The healthcare industry also struggles with maintaining and achieving a cybersecurity plan that strives for longstanding improvements on their technological devices and systems. According to Claire Jarvis (2019), outdated IT infrastructure may form as the result of the ‘break-fix’ mindset where hospital administrators repair IT systems after they are broken opting for a short-term solution instead of conducting consistent, preventative maintenance that would prove better for long-term improvements. The break-fix method creates an unbreakable cycle that does not prioritize keeping IT infrastructure current and updated.

Healthcare IoT Raises Data Privacy Concerns

The interconnectedness of medical IoT devices raises concerns surrounding data privacy. Such concerns include risks of patients' privacy exposure through data eavesdropping and location privacy. This section will examine each of these concerns while also identifying key stakeholders that should be held accountable for data privacy in IoT devices.

The first data privacy concern associated with IoT devices in healthcare is the risk of exposing patient information. Healthcare organizations have a responsibility to keep patients' Personal Health Records confidential. According to Mayo Clinic (2020), a Personal Health Record (PHR) is simply "a collection of information about a patient's health" and can either be traditional paper records or electronic (para. 2). PHRs contain personal and private information that is drawn from multiple health sources to build a comprehensive health file (Sciforce, 2019). The confidential nature of PHRs leaves them as attractive targets for cybercriminals who want to steal consumer data and information. Electronic Protected Health Information (e-PHI) is also collected from healthcare IoT devices and stored in PHRs. Examples of e-PHI taken from IoT devices can include blood pressure, heart rate, glucose levels, and even drug efficacy. Bad actors that intercept e-PHI records can carry out malicious activities that puts the privacy of patients at risk. Many times, cybercriminals will post and sell patients' e-PHI on the dark web for hundreds of dollars (Check Point, 2020).

Location privacy is another concern related to IoT devices in healthcare. There is a concern that cybercriminals could eavesdrop on a patient's location through the IoT devices that they are required to wear on a continuous basis and cannot take the devices off without the permission of their health professional. As per Ugrenovic and Gardasevic (2015), the critical parts of IoT architecture are Wireless Sensor Networks (WSNs) which are made up of lowpower sensors that collect and send data through a gateway to the outside world. In IoT healthcare devices, “WSNs provide useful applications such as patient monitoring in real time, drug administration, help in diagnostics, and tracking patients inside the hospital” (Ugrenovic & Gardasevic, 2015, p. 1). WSNs can also use their sensors to send location data to the patient’s health facility along with remote monitoring of the patient. Professionals have found WSNs to exhibit location privacy issues due to insecure gateways and reverse engineering tactics by cybercriminals.

While many may argue that data privacy is solely the responsibility of the entity that is distributing the IoT devices to consumers, responsibility falls on many other entities as well. Perera et al. (2015) identified and described five major stakeholders that are responsible for protecting user privacy:

- **Device manufacturers**: device manufacturers are responsible for embedding and implementing privacy techniques, such as secure storage, data deletion, and access control mechanisms into their devices while also explaining how and when consumer data would be extracted from the devices.
- **IoT cloud services and platform providers**: cloud providers are responsible for using common standards, interfaces, and data formats so consumers can choose which provider they want to use, along with seamlessly moving data from one provider to another when necessary.
- **Third-party application developers**: third-party application developers are first responsible for ensuring that their apps do not contain any malware. It is also their responsibility to present accurate information to consumers about the data and information they are going to collect to receive explicit user consent. In the case of IoT,

user consent should be an ongoing and repetitive process since these IoT devices are regularly gathering data.

- **Government and regulatory bodies**: government and regulatory bodies are responsible for creating and implementing standards and legal efforts that hold parties accountable for their actions. It is important to note that the goal of standards is not to limit innovation, but rather to ensure interoperability between IoT solutions.
- **Individual consumers and non-consumers**: IoT device owners have a responsibility to themselves and others to "notify non-consumers regarding the nature of the solutions deployed and related information" (Perera et al., 2015, p.37). Most often, non-consumers do not realize they can be indirectly affected by IoT devices.

By considering all the major stakeholders involved in manufacturing, deploying, and using IoT devices, user privacy can be better protected and enforced. Better user privacy will bring various advantages, such as increasing consumer confidence and reducing the risk of cyber threats.

COVID-19 Increases Cybersecurity Concerns in Healthcare IoT

As cases of COVID-19 spiked in early 2020, healthcare facilities were severely affected by the influx of new patients and their capacity to treat them with limited resources. At the same time, IT administrators in hospital facilities had to quickly adapt to the increasing number of medical devices connected to their network while balancing how to secure these devices. With even more devices connected to the network, cybersecurity risks increased on an unprecedented level (Langer, 2020). This is especially a problem if healthcare IoT devices are not updated or patched to the latest security standards. In a research study conducted by Bitdefender, "the number of cyberattacks detected at hospitals in March 2020 increased by almost 60 percent from February" (Arsene, 2020). Research suggests that cybercriminals are using COVID-19 as an opportunity to take advantage of a fearful situation and wreak havoc on health organizations and individuals alike.

COVID-19 made and continues to make devastating impacts on all aspects of society, and healthcare seems to have taken the biggest hit. Various effects caused by COVID-19 have contributed to some of the most challenging cybersecurity issues. As per Lerman (2020), these effects include the following:

- **Understaffed hospitals**: budget cuts, lay-offs, and an economic downfall led to decreased number of workers, such as IT and cybersecurity professionals in the workplace.
- **Adoption of remote work and telehealth**: the sudden switch to telehealth to protect both patients and health professionals led to a greater attack surface for unsecure devices, systems, and networks that are susceptible to intrusion.
- **Equipment shortages**: along with the surge of patients being in hospitals, the number of required IoT devices have also increased. Many of these devices become connected to the healthcare network before going through proper cybersecurity assessments.

With sudden social distancing regulations that required people to stay home, hospitals had to turn to telehealth services to provide medical care. As part of telehealth services, healthcare organizations implemented remote patient monitoring (RPM) systems for patients that require continuous observation from the safety of their home. According to Jackson (2020), “the goal of any telehealth or RPM solution is for clinicians to have access to timely and reliable patient data which can be used to make appropriate clinical decisions” (para. 4). An RPM device essentially functions as an endpoint that connects the patient to their healthcare provider. As endpoint devices are interconnected, any device that is not cyber secure poses as a vulnerability that could have ripple effects on the entire network if it gets infected (Jackson, 2020). Patients' homes also pose as locations that may have weak network infrastructure in comparison to a health organization. Many of these patients do not have a comprehensive understanding of cybersecurity awareness, such as implementing two-factor authentication, data encryption, and password security, so vulnerabilities are endless. Patients may also have various technologies on their network, such as routers, switches, smartphones, tablets, etc., and there is no guarantee that their devices are secure.

How Medical IoT Devices Are Susceptible to Cyber Attacks

With the advancement of medical technology comes waves of cyber attacks and threats. More healthcare organizations are starting to distribute medical IoT devices to their patients to efficiently monitor their health and make timely decisions. With more IoT devices interconnected through different networks, the risk of a cyber threat increases which could put a patient's health or life in danger.

As per O'Brien et al. (2018), known threats that can affect medical IoT devices include: targeted attacks, advanced persistent threats, denial-of-service attacks, malware infections, theft, and misuse. These cyber threats take advantage of the devices' vulnerabilities, such as misconfiguration, outdated software, and lack of encryption both at rest and in transit (O'Brien et al., 2018).

The most popular medical IoT devices given to patients are wireless infusion pumps. According to Langston (n.d.), infusion pumps are used to "remotely manage and administer blood, saline, and other medical fluids" and "make up over half of all medical IoT devices deployed today" (para. 1). Wireless infusion pumps have various benefits, such as decreasing costs, increasing efficiency, and assuring better quality of patient care (Langston, n.d.). While these devices offer advantages, there are cybersecurity concerns surrounding the wireless connectivity that connects the pump to the health facility’s medication system and electronic health records. Hacking an infusion pump and modifying dosages of medicine could lead to deadly health issues, like an overdose (Waqas, 2018). A group of doctors at RSA 2018, a popular cybersecurity conference, simulated this exact situation to demonstrate how serious this situation would be (Waqas, 2018). Similarly, in 2016, “a group of researchers hacked a connected pacemaker and found several potentially life-threatening vulnerabilities due to poor authentication and encryption practices” (Sciforce, 2019, para. 2). Making medical IoT devices cyber safe must become a part of health organizations’ priorities, especially as these attacks can threaten patient safety.

The Solution

While there is no exact technique to stop all cyber threats and attacks, there are steps healthcare facilities can take to reduce and prevent cyber risks and vulnerabilities. This research will offer a few specific solutions to address the problems mentioned above. The first solution will discuss an enterprise risk management (ERM) approach to IoT in healthcare. By using ERM, Chief Risk Officers (CRO) and Chief Information Security Officers (CISO) can incorporate a holistic approach to identify, assess, control, and review cyber risks associated with IoT. This research will also investigate the integration of risk management frameworks and techniques as a critical step in mitigating cyber risks. The second solution will involve understanding how network segmentation of IoT devices in healthcare can reduce cyber risks and threats. Finally, the third and final solution will involve detailed research and investigation on various standards, laws, and regulations that discuss cybersecurity for IoT devices in healthcare. This may include standards that require IoT manufacturers to regularly release patches and software/hardware updates, along with any laws or regulations related to protecting consumers' private information.

Integrating Risk Management into Healthcare IoT

One solution for managing IoT in healthcare is to use risk management concepts and techniques to effectively secure IoT devices on a larger scale. Healthcare organizations can use risk management frameworks, along with governance, risk, and compliance (GRC) to begin building or modifying their current cybersecurity infrastructure to effectively address their cybersecurity concerns. Furthermore, healthcare entities need to use cyber risk strategy to understand how healthcare is transforming on a digital scale, along with how cybersecurity fits into their overall goals (AT&T, 2020).

The risk management process helps companies organize their assets to recognize which assets need further protection. The source and impact of different risks vary among different organizations; for example, some risks stem from human error, while others stem from system error depending on how well an organization protects its assets. According to the CRO Forum (2014), cyber risk is any potential source of loss within a cyber environment. Cyber risks can emerge from Internet use, electronic data transmission, physical damage, data storage, and the CIA triad of electronic information. Different implementations of business policies, such as bring-your-own-device, mobile use, cloud traffic, and the Internet of Things, can also impact cyber risk (CRO Forum, 2014).

This section will provide an example of analyzing healthcare IoT devices using cyber risk management through an enterprise risk management approach. Enterprise risk management evaluates the relationship between different risks and how they all communicate and interact. The first step in the risk management process is to identify assets and potential risks. Loss exposure checklists, flowcharts, and financial contract analyses assist risk managers with this process. In healthcare, IT administrators can identify and track all the IoT devices they have in stock or have distributed to patients. Once the assets and risks are identified, risk professionals evaluate and score the frequency and severity of each risk using statistics. IoT devices can be ranked depending on how severe and frequent the cyber risk associated with each asset is. Ranking risks helps organizations choose which risk management techniques to implement, which is the third step of the process. Risk management techniques include risk control, financing, avoidance, retention, and transfer. If an IoT devices becomes defective or infected with malware, then healthcare organizations can use risk management techniques, such as buying insurance or paying out of pocket for replacing damaged devices. Finally, the last step in the risk management process is to review and implement decisions while considering risk changes over the company's lifetime. Healthcare facilities can consider how their long-term goals are changing, along with how cybersecurity risks are continuously evolving.

One popular risk transfer technique is insurance. This involves an organization purchasing a policy to transfer certain risks to an insurance company. Insurance mainly assists with risks that rarely occur but would severely impact the organization. Cyber risks are difficult to manage due to a shifting cyber threat landscape, complex interconnectivity between companies and individuals, and scattered data loss (CRO Forum, 2014).

A cyber risk that could affect healthcare IoT devices is a data breach. Data breaches impact organizations and consumers alike. To transfer sections of this risk, organizations can buy first- and third-party cyber liability insurance. First-party cyber insurance covers losses the policyholder directly suffers, like theft, business interruption and physical damage, while third-party insurance "covers claims and damages caused by another party" (Black et al., 2018, p. 6).

According to OECD (2017), standalone cyber policies can vary, as organizations can cater policies to insure severe risks. Stand-alone cyber insurance policies can cover data confidentiality breaches that accumulate the following items: incident response costs, legal costs, fines, penalties, breach of privacy compensation, and extortion.

Implementing Network Segmentation of Healthcare IoT Devices

Another solution for securing IoT in healthcare includes network segmentation. IoT devices are especially susceptible to infiltration due to the lack of security embedded in them when they are released; for example, many IoT devices lack proper encryption standards and cannot properly filter the traffic that comes in and out of the device (Craven, 2020). Network segmentation is cited as a best practice in NIST SP800-125 (Wolf, 2019). David Wolf (2019), the Principal Security Researcher for *Firescout*, emphasizes that while network segmentation is not the ultimate solution to solving cybersecurity risks, it can provide an organization with a better defensive strategy when used in combination with other security strategies.

Network segmentation involves the process of "dividing a network into subnets [to] improve network performance and enhance security (Hadaegh, 2019, para. 5). Segmentation allows IT administrators to split network traffic between internal and external users and confines the flow of traffic between policy-based groups that can enforce rules and privileges based on device profiles (Hadaegh, 2019).

The primary benefit of using network segmentation is that if one device on an organization's network becomes infected, then the infection is limited in its ability to infect other devices in the network (Wolf, 2019). In the case of healthcare IoT, IT administrators may choose to separate hospital-owned devices from patient and employee-owned devices to limit the risk of an infected device spreading to other nodes on a network (Wolf, 2019). Wolf (2019) further asserts that if an anomaly device is spotted on the network, then network segmentation can help law enforcement trace back a cyber attack to the initial point of entry.

Standards, Laws, and Regulations

The introduction of IoT devices into healthcare is a relatively new concept, so legal standards, laws, and regulations mainly related to the internal architecture and security of these devices is critical. These legal statures help ensure that consumers' privacy and security is protected, fraudulent activity is reduced, and data systems are improved. By understanding cybersecurity compliance requirements, healthcare organizations can reduce security risks that can otherwise turn into disaster.

The most well-known law associated with protecting patient information is the Health Insurance Portability and Accountability Act (HIPAA). According to the CDC (2018), HIPAA became a law in 1996 and "required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge" (para. 1). To implement the requirements outlined in HIPAA, the U.S. Department of Health and Human Services (HHS) released the HIPAA Privacy and Security Rules (CDC, 2018). While the Privacy Rule guards protected health information (PHI), the Security Rule specifically protects electronic PHI (e-PHI) that could be created, stored, received, or transmitted (CDC, 2018).

The HIPAA Security Rule requires entities handling e-PHI to follow key cybersecurity techniques such as the following (CDC, 2018):

- Ensure the confidentiality, integrity, and availability of e-PHI
- Detect and protect against cybersecurity threats that can endanger e-PHI
- Protect against unauthorized access to e-PHI or prohibited use
- Verify compliance with national standards

These safeguard cybersecurity techniques are not solely technical in nature. As per the American Medical Society (n.d.), there are administrative, physical, and technical safeguards that healthcare organizations can use to protect e-PHI and ensure compliance with HIPAA.

As discussed in the previous section, risk management is a great tool to identify, rank, and assess cybersecurity risks. e-PHI is a highly valued asset found in healthcare IoT devices that healthcare organizations cannot afford to let cybercriminals steal and sell. To maintain compliance with HIPAA, entities are required to conduct regular risk assessments to determine their main threats to e-PHI and create a documented plan to mitigate such threats.

While laws like HIPAA do protect e-PHI in general, there are fewer laws, standards, and regulations that outline who is responsible for protecting e-PHI specifically in IoT devices (Kirk, 2019). Such ambiguity highlights the need for more specific legislation that outlines which parties are responsible for protecting devices and who should be held accountable for mishaps. As part of the initiative to secure IoT, both the House and Senate recently passed the IoT Cybersecurity Improvement Act to now be sent to the president for approval (O’Donnell, 2020). O’Donnell (2020) states that if approved, this law would require IoT vendors and manufacturers to meet basic security requirements while conforming to existing standards and best practices. This is a groundbreaking step in improving the overall quality of IoT devices in both the private and public sector.

Conclusion

Society has made great strides in technology, making everyday tasks efficient and effective. The Internet of Things (IoT) is one technology that has been significantly increasing in every sector, especially healthcare. Over time, the adoption of IoT devices into healthcare settings has escalated the number of cybersecurity risks and threats that continue to affect organizations and individuals. Healthcare IoT presents different cybersecurity concerns, like data privacy, outdated systems, and the trickling effects of COVID-19. While there are many problems associated with healthcare IoT, organizations can take different steps to mitigate cyber risks and threats, such as using risk management, network segmentation, and legal statures. While the solutions mentioned in this paper emphasize best practices that are already in use today, organizations can investigate innovative and proactive methods to secure their IoT devices. One innovative solution includes designing a tool that uses machine learning or artificial intelligence to detect the early stages of a cyber attack and use automated tools to stop the perpetrator. Using both offensive and defensive cybersecurity measures is necessary in staying one step ahead of cybercriminals, especially in the healthcare sector. Healthcare is an ever-growing industry and it is vital that people recognize how essential cybersecurity efforts are in protecting data, information, networks, systems, and people.

References

American Medical Association (n.d.). *HIPAA security rule & risk analysis*. https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis

Arampatzis, A. (2019, June 19). *Cyber security challenges in healthcare IoT devices*. Tripwire. https://www.tripwire.com/state-of-security/security-data-protection/iot/cyber-security-healthcare-iot/

Arsene, L. (2020, May 13). *Global ransomware and cyberattacks on healthcare spike during pandemic*. Bitfender. https://labs.bitdefender.com/2020/05/global-ransomware-and-cyberattacks-on-healthcare-spike-during-pandemic/

AT&T (2020). *Healthcare and Cybersecurity: Helping protect the digital transformation*. https://www.business.att.com/content/dam/attbusiness/infographics/att-cybersecurity-and-healthcare-ebook.pdf

Black, D., Margolis, K., Milam, G., & Ruzic, E. (2018). *A guide to cyber insurance*. The Risk Management Society. http://www.rims.org/resources/risk-knowledge/white-paper/a-guide-to-cyber-insurance

CDC (2018, September 14). *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. https://www.cdc.gov/phlp/publications/topic/hipaa.html

Check Point Software Technologies Ltd. (2020). *Check Point IoT protect for healthcare*. https://www.checkpoint.com/downloads/products/cp-iot-security-healthcare-solution-brief.pdf

Craven, C. (2020, June 2). *How is the Internet of Things (IoT) vulnerable*? Sdx Central. https://www.sdxcentral.com/5g/iot/definitions/how-is-internet-of-things-iot-vulnerable/

CRO Forum. (2014). *Cyber resilience: The cyber risk challenge and the role of insurance*.

https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf

Donovan, F. (n.d.). *Outdated healthcare IT infrastructure can weigh down organizations*. HIT Infrastructure. https://hitinfrastructure.com/news/outdated-healthcare-it-infrastructure-can-weigh-down-organizations

Hadaegh, H. (2019, January 16). *Tame IoT threats with network segmentation*. IBSS. https://www.ibsscorp.com/blog/cybersecurity/taming-iot-threats-with-network-segmentation

Haughey, J., Taylor, K., Dohrmann, M., & Snyder, G. (2018). *Medtech and the Internet of Medical Things*. Deloitte. https://www2.deloitte.com/global/en/pages/life-sciences-and-healthcare/articles/medtech-internet-of-medical-things.html

Hill, M. (2020, February 20). *Security by sector: Medical IoT gets much needed dose of cybersecurity*. Infosecurity Magazine. https://www.infosecurity-magazine.com/blogs/medical-iot-cybersecurity/

Hung, M. (Ed.). (2017). *Leading the IoT: Garner insights on how to lead in a connected world.* Gartner. https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

Jackson, G.W. (2020, March 18). *Security considerations for deploying telehealth and remote patient monitoring systems*. Clearwater Compliance. https://clearwatercompliance.com/blog/security-considerations-for-deploying-telehealth-and-remote-patient-monitoring-systems/

Jarvis, C. (2019). *Aging hospitals aren't ready for the technology revolution*. Salon. https://www.salon.com/2019/12/21/opinion-aging-hospitals-arent-ready-for-the-technology-revolution_partner/

Kirk, C. (2019, June 11). *Healthcare IoT adoption in the HIPAA compliance landscape.* LightEdge. https://www.lightedge.com/blog/healthcare-iot-adoption/

Langer, J. (2020, August 10). *Four healthcare security lessons learned during the initial COVID-19 surge*. Security Magazine. https://www.securitymagazine.com/articles/93028-four-healthcare-security-lessons-learned-during-the-initial-covid-19-surge

Langston, F. (n.d.). *Top 6 hackable medical IoT devices*. CI Security. https://ci.security/resources/news/article/top-6-hackable-medical-iot-devices

Lerman, L. (2020, July 06). *COVID-19: What healthcare IoT cyber security learned from the first wave*. IoT Now. https://www.iot-now.com/2020/07/06/103739-covid-19-what-healthcare-iot-cyber-security-learned-from-the-first-wave/

Matthews, K. (2018, December 27). *5 challenges facing health care IoT in 2019*. IoT For All. https://www.iotforall.com/5-challenges-facing-iot-healthcare-2019

Mayo Clinic (2020, July 02). *Personal health records and patient portals*. Mayo Clinic. https://www.mayoclinic.org/healthy-lifestyle/consumer-health/in-depth/personal-health-record/art-20047273

Morgan, S. (2019). *2019/2020 cybersecurity almanac: 100 facts, figures, predictions and statistics.* Cybercrime Magazine. https://cybersecurityventures.com/cybersecurity-almanac-2019/

Noble, O. (2020, September 30). *UHS cyberattack: Why health care is a vulnerable target*. Medical Economics. https://www.medicaleconomics.com/view/uhs-cyberattack-why-health-care-is-a-vulnerable-target

O’Brien, G., Edwards, S., Littlefield, K., McNab, N., Wang, S., & Zheng, Kangmin. (2018, August). *Securing wireless infusion pumps in healthcare delivery organizations*. National

Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1800-8

O'Donnell, L. (2020, November 19). *IoT Cybersecurity Improvement Act passed, heads to President's Desk*. Threatpost. https://threatpost.com/iot-cybersecurity-improvement-act-passed/161396/

OECD. (2017). *Enhancing the role of insurance in cyber risk management*. https://dx.doi.org/10.1787/9789264282148-en

Perera, C., Ranjan, R., Wang, L., Khan, S. U., & Zomaya, A. Y. (2015). Big Data Privacy in the Internet of Things Era. *IT Professional*, *17*(3), 32–39. https://doi.org/10.1109/MITP.2015.34

Sciforce (2019). *Ensuring privacy and security in the healthcare IoT*. Medium. https://medium.com/sciforce/ensuring-privacy-and-security-in-the-healthcare-iot-7b97549d629c

Tankovska, H. (2020). *Internet of Things - active connections worldwide 2015-2025*. Statista. https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/#statisticContainer

Ugrenovic, D., Gardasevic, G. (2015). CoAP protocol for Web-based monitoring in IoT healthcare applications. *23rd Telecommunications Forum Telfor (TELFOR).* https://www.researchgate.net/publication/280023498_IoT_Wireless_Sensor_Networks_for_Healthcare_Applications

Waqas. (2018, April 20). Medicine pumps & pacemaker threat as Dr's simulate hacked overdose. HackRead. https://www.hackread.com/medicine-pumps-pacemaker-threat-hacked-overdose/

Wolf, D. (2019, October 16). *Network segmentation is a security best practice, but is adoption lagging in healthcare?* Forescout. https://www.forescout.com/company/blog/network-segmentation-is-a-security-best-practice-but-is-adoption-lagging-in-healthcare/