Securing Consumer Mobile Healthcare Devices

2021 Public-Private Analytic Exchange Program

Vulnerabilities in Healthcare Information Technology Systems

Acknowledgements

We acknowledge and thank the Federal government agencies and companies that supported the development of this paper. We also thank the Office of the Director of National Intelligence (ODNI) and the US Department of Homeland Security (DHS) for the opportunity to have participated in the 2021 Public-Private Analytic Exchange Program (AEP).

People and Organizations Consulted

During developing this paper, several individuals were consulted to inform the team of risks and approaches in safeguarding consumer health technology. While the group represents subject matter experts from organizations with experience in this topic, the opinions offered represent those from the individuals, rather than representing viewpoints from their respective organizations. We are grateful to the individuals that provided their time to advise, answer questions, and assist in the developing the report.

- Dr. Synho Do- Harvard Medical School
- Matilde Grecchi - Head of Data Science & Innovation - Analytics & Innovation Lab Zucchetti
- Amyn Jan; Chief Strategist; US Government
- Lee Kim
- Matthew Rosenquiste: CISO at Eclipz
- Axel Wirth, Chief Security Strategist, MedCrypt

Public/Private Team Members

- Jenifer Clark, Costco Wholesale
- Joyce Clutter, Department of Veteran Affairs
- Chandra Pauline Daniel, New York Medical College
- Bruce de'Medici, Grey Oar
- Joe D., Department of Justice
- Christopher Letterman, Wostmann and Associates
- Kevin Littlefield, MITRE Corporation
- Hany Wassef, Meritor
- Michele Krajewski, AEP Team Champion, Department of Veterans Affairs

Executive Summary

Technology advances empower consumers with sophisticated capabilities, allowing them to be active participants in managing their health. Consumers benefit from healthcare technology that is easily accessible and offers health data visibility that, until recently, was available only to or through healthcare providers. However, consumer healthcare technology is not subsumed within medical technology; the safeguard landscape for the design and production of consumer healthcare products and medical devices is not identical. Consumer healthcare technology manufacturers may not be subject to the same regulatory requirements as medical device manufacturers and may not integrate consumer safeguards into their design and production with the same priorities as medical device producers. Thus, consumer healthcare technology has similar attributes to smart phone devices or other "Internet of Things" endpoints that are not developed within a medical safety landscape. This paper surveys the privacy and security landscape impacting upon use of wearable consumer healthcare technology and leverages mitigation approaches based on established practices that are extant for use of other technology.

Securing Consumer Mobile Healthcare Devices

I. Introduction

"Consumer healthcare technology empowers consumers to become active participants in their overall healthcare management by offering cost-effective and sophisticated technology. However, manufacturers may not implement sufficient privacy and security controls on the devices, or measures to protected aggregated data." - Department of Homeland Security (DHS) Analytic Exchange Program (AEP) Vulnerabilities in Healthcare Information Systems team statement.

Wearable healthcare technologies can be innovative solutions for healthcare problems. They enable continuous monitoring of human physical activities and behaviors, as well as physiological and biochemical parameters during daily life. A 2018 literature review of wearable technology healthcare applications, published on the Healthcare Information and Management Systems Society (HIMSS) website[1], identified over 60 papers on wearable technologies being developed for disease prevention and health maintenance, patient management, and disease management. Most of the wearable technologies that they found were still in the prototype stage, but security and privacy issues and concerns were identified as one of the barriers to future adoption, especially in the area of Health Insurance Portability and Accountability Act (HIPAA) compliance.

According to the Trusted Connectivity Alliance,[2] wearable technology includes several technical, logistic and security requirements. Wearable technology should:

- Have flexible and/or standalone connectivity with standalone connectivity being a key consideration,
- Protect the privacy of the sensitive, high-value user data they collate, store, and transmit,
- Protect the integrity and accuracy of user data that is stored and transmitted,
- Ensure the integrity and authenticity of the software/firmware through malware protection,
- Ensure end-user convenience and flexibility by allowing them to manage mobile subscriptions across multiple devices, and
- Provide ways to protect stored data in the case where the device is lost or stolen.

This white paper explores wearable technology security and privacy challenges and discusses tools and information that may exist to help consumers to mitigate those challenges.

[1] Wu, M., PhD, Luo, J., PhD; Online Journal of Nursing Informatics Contributors. Wearable Technology Applications in Healthcare: A Literature Review | HIMSS. Published November 25, 2019. Accessed July 6, 2021. https://www.himss.org/resources/wearable-technology-applications-healthcare-literature-review

[2] Wearable Devices. Trusted Connectivity Alliance. Accessed July 6, 2021. https://trustedconnectivityalliance.org/wearable-devices/

II. Security and Privacy Risks and Challenges of Wearable Healthcare Devices

When consumers use wearable healthcare devices, the technology needs to assure appropriate data protection. Wearable healthcare devices should include capabilities that assure security and privacy controls that protect the data that the device collects, stores, and transmits. At the same time, device manufacturers should maximize device use flexibility and convenience to the consumer. The following describes a few of the security and privacy considerations inherent in wearable healthcare devices:

Limiting the use of user data

With the rise in the use of wearable healthcare devices that track health and wellness activities, there has been a corresponding rise in the use of these devices by employers to incentivize and measure participation in workplace wellness programs. As individuals adopt wearable device usage, sensitive health-related or personal data may be created. Privacy and security controls may not be present in these programs, and data governance programs may be unclear, without a clearly established regulatory obligation that provides guidance on safeguarding the data. For example, programs offered to all employees may not fall under the purview of the Health Insurance Portability and Accountability Act (HIPAA) and therefore compliance requirements with the HIPAA Security and Privacy rules may not be defined clearly, or not applicable. Some of these programs link back directly to health insurance companies and employers with the data being used in determining healthcare premiums.[3]

Inadvertent disclosure of ancillary information

Users of wearable healthcare devices often share information gathered by those devices without realizing how that data could be used to discover information that they do not intend to share. An example of this came to light in 2018 when the global heat map created by Strava, a fitness tracking app used by military personnel in Iraq, was shown to reveal the location of several U.S. military strongholds. Security experts also speculated that the user-generated map could not only show the locations of military bases, but specific routes most heavily traveled as military personnel unintentionally shared their jogging paths and other routes.[4]

Innovation outpacing security

The popularity of wearables, such as fitness trackers and smart watches, is growing at a staggering rate but the security of these wearables is not keeping up. The increase in the number of native applications available for smartwatches will create new opportunities for fraudsters to compromise wearable healthcare devices for access to highly valuable personal information.[5]

Unauthorized use and sale of data by data brokers

The ambiguity in the terms of use for wearables is used to reserve some actions with "third parties" also known as data brokers. The US Federal Trade Commission (FTC) released a report to Congress in May 2014 after an in-depth study of nine data brokers. The report revealed that these companies acquired data from various sources, including wearables, to be sold in packages to companies with diverse interests, all private and lucrative. In 2012, these businesses invoiced $426 million within the US. Although regulations

[3] What You Need to Know About Data Security and Wearable Devices in the Workplace. WEX Inc. Published February 5, 2018. Accessed July 6, 2021. https://www.wexinc.com/insights/blog/health/what-you-need-to-know-about-data-security-and-wearable-devices-in-the-workplace/

[4] Molina, B., Jan 29, 2018. Strava map fallout: How much do you know about your fitness app's tracking? USA TODAY. Accessed July 9, 2021. https://www.usatoday.com/story/tech/news/2018/01/29/strava-map-fallout-how-much-do-you-know-your-fitness-apps-tracking/1074475001/

[5] Shepard, S., Jul 30, 2018. Wearables Open Door to Many Security Vulnerabilities - Security Today. Accessed July 6, 2021. https://securitytoday.com/articles/2018/07/30/wearables-open-door-to-many-security-vulnerabilities.aspx

are in place in almost all parts of the world that moderately protect the digital consumer from apathy when being made aware about what information is shared, the wearable healthcare devices data highway assumes a free hand to an abundance of data for these companies.[6]

Data is vulnerable in transit

Wearable healthcare devices are dependent on underlying operating systems and software. Two popular mobile device operating systems are iOS (iPhone OS) and Android. Smart cellular phones and tablets use these operating systems. Wearable healthcare devices may be "tethered" to a smart phone or a tablet, for example, for network communications capabilities, or may use these operating systems to support the wearable device's software. Operating systems may include vulnerabilities that are targeted by hackers. Successful vulnerability exploitation may expose private data.

With wearable healthcare devices, consumers may be limited in controlling or imposing limits on the wearable device's data collection process. Consumers may not have the option to shut down a wearable device's sensors individually or cancel the device's data collection. Consumers may find it difficult to limit a device manufacturer or other parties from viewing or using collected data. Further, device manufacturers may not implement appropriate data-in-transit protections.[7]

Lack of industry standards, laws, and regulations

The data transmission formats, encryption and confidentiality, integrated platform interfaces, and data transmission protocols generated by various devices lack uniform industry standards, and a series of problems such as information silos and privacy protection have emerged. There is also no uniform industry standard for the data format and content collected by healthcare wearable healthcare devices, creating difficulties in the storage and management of data as well as integration and utilization of data. Additionally, there is a lack of cohesive federal policies and regulations on data security and privacy protection for wearable healthcare devices, including healthcare wearable healthcare devices. Certain uses of wearable healthcare devices don't fall under HIPAA regulations, allowing wearable device manufacturers to sell user data.[8]

For additional information on regulatory gaps, security concerns, and recommendations, see Montgomery K.C., Chester J., Kopp K.; "Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection" https://www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf and the HHS Cybersecurity Program briefing on Wearable Device Security; https://www.hhs.gov/sites/default/files/hc3-intelligence-briefing-wearable-device-security.pdf.

III. Securing Wearable Healthcare Devices

Consumers

Wearable healthcare devices may interoperate with a consumer's smart phone device. Consumers should ensure that they apply appropriate cyber hygiene practices on mobile devices such as their smart

[6] Shepard, S., Jul 30, 2018. Wearables Open Door to Many Security Vulnerabilities - Security Today. Accessed July 6, 2021. https://securitytoday.com/articles/2018/07/30/wearables-open-door-to-many-security-vulnerabilities.aspx

[7] Jiang, D., Shi, G., Feb 08, 2021. Research on Data Security and Privacy Protection of Wearable Equipment in Healthcare. *Journal of Healthcare Engineering*. 2021;2021:e6656204. doi:10.1155/2021/6656204, https://www.hindawi.com/journals/jhe/2021/6656204/

[8] Jiang, D., Shi, G., Feb 08, 2021. Research on Data Security and Privacy Protection of Wearable Equipment in Healthcare. *Journal of Healthcare Engineering*. 2021;2021:e6656204. doi:10.1155/2021/6656204, https://www.hindawi.com/journals/jhe/2021/6656204/

phone device.[9] Consumers may find smart phone security guidance by leveraging tools offered by the Federal Communications Commission (FCC). For example, the FCC implemented FCC Smartphone Security Checker.[10] This FCC website provides a tool that smartphone users can use to secure their phones. Consumers may navigate the website's interface, select a mobile device operating system, and then click on the "Generate Your Checker" button.

While cursory searching may identify that mobile and wearable device pose challenges to consumers, device manufacturers may be remiss in proactively providing privacy and security measures. Device safeguarding guidance is available. This paper identifies several links that may serve as starting points for consumers that need information on securing their devices. Some common approaches are as follows:[11] [12] [13] [14] [15] [16]

- Use the passcode lock on smartphone, smartwatch, and other devices. This will make it more difficult for thieves to access information if a device is lost or stolen;
- Protect a smart phone from viruses and malicious software, or malware, as one would do for a workstation by installing mobile security software;
- Use caution when downloading apps. Consumers should avoid third-party apps (*e.g.*, apps not purchased through a trusted or managed application distribution store). Apps can contain malicious software, worms, and viruses. Consumers should beware of apps that ask for unnecessary "permissions.";
- Delete apps that are not needed;
- Check the privacy setting on any apps that collect personal data and limit what gets shared. Consumers should limit sharing between apps;
- Limit location permissions;
- Apply caution when using social network accounts to sign into apps;
- Keep your software/firmware updated on your phone, mobile apps, and wearable healthcare devices;
- Avoid storing sensitive information like passwords or a social security number on your mobile device;
- Beware of "shoulder surfers" or other social engineering tactics. A common form of information theft is observation. Consumers should beware of your surroundings especially when you are punching in sensitive information.

[9] 4 tips for better smartwatch security | ExpressVPN. Home of internet privacy. Published January 5, 2021. Accessed July 12, 2021. https://www.expressvpn.com/blog/smartwatch-security/
[10] FCC Smartphone Security Checker. Federal Communications Commission. Published October 30, 2015. Accessed July 6, 2021. https://www.fcc.gov/smartphone-security
[11] https://www.first1bank.com/_/kcms-doc/355/31654/Tips-to-secure-your-mobile-device.pdf
[12] 4 tips for better smartwatch security | ExpressVPN. Home of internet privacy. Published January 5, 2021. Accessed July 12, 2021. https://www.expressvpn.com/blog/smartwatch-security/
[13] Security Considerations for Wearable Technology. Accessed July 6, 2021. https://platinumdatarecovery.com/blog/security-considerations-for-wearable-technology
[14] Safeguarding Against Hackers is Necessary to Secure the Future of Medical Wearable Technology. UL. Accessed July 6, 2021. https://www.ul.com/news/safeguarding-against-hackers-necessary-secure-future-medical-wearable-technology
[15] Phone Security: 20 Ways to Secure Your Mobile Phone. The Missing Report. Published April 6, 2021. Accessed July 6, 2021. https://preyproject.com/blog/en/phone-security-20-ways-to-secure-your-mobile-phone/
[16] How To Protect Your Privacy on Apps. Consumer Information. Published May 11, 2021. Accessed July 6, 2021. https://www.consumer.ftc.gov/articles/how-protect-your-privacy-apps

- Wipe your mobile device before you donate, sell, or trade it using specialized software or using the manufacturer's recommended technique;
- Enable settings that deter theft. Some mobile device features allow the consumer to wipe your device remotely if it is lost or stolen;
- Beware of mobile phishing. Avoid opening links and attachments in emails and texts, especially from unknown senders;
- Apply caution when using public Wi-Fi connections. Public Wi-Fi access points may not promote appropriate security measures and using public Wi-Fi access points may result in exposing sensitive data;
- When available, enable data encryption (data-at-rest protection) and use two-factor authentication or security keys to access network services and applications.

Remanufacturing and Servicing

The FDA has also taken steps to provide guidelines appliable to servicing or remanufacturing medical devices. In the proposed guidelines, the FDA recognizes that medical devices are often reusable and need preventive maintenance and repair during their useful life. Recognizing that remanufacturing has implications for specific regulatory responsibilities and direct impact upon safety of the ultimate user of the medical device, the FDA issued the draft guidelines to help clarify when remanufacturing is occurring. In the draft, the FDA defines (i) remanufacturing as processing, conditioning, renovating, repackaging, restoring, or other changes to a finished device that significantly changes the devices' performance safety specifications or intended use and (ii) servicing as repair or preventive or routine maintenance of one and more parts in a device after distribution.[17] These guidelines can be applied for wearable healthcare devices.

Safer Technologies Program (STeP)

The FDA has also implemented STeP to provide a collaborative opportunity for manufacturers of medical devices that are expected to significantly improve safety of currently available treatments or diagnostics targeting certain diseases or conditions that are generally non-life threatening or reversible. To be eligible, the medical devices must be subject to a pre-market approval, de novo classification request, or premarket notification. The FDA's intent is to allow manufacturers of those devices to interact with FDA experts to address topics as they arise during pre-market review phase and improve the efficiencies of those communications. The FDA's goal in the STeP program is to facilitate delivery of qualified medical devices to end users more quickly by expediting their development, assessment, and review while also preserving statutory standards for their delivery to the market. These guidelines can also be applied for wearable healthcare devices.

IV. Cybersecurity of Medical Devices

NIST standards

In May 2020, the National Institute of Standards and Technology (NIST) issued standards to provide organizations with a starting point to use in identifying device cybersecurity capabilities for new IOT devices that they manufacture, integrate, or acquire. (NISTIR 8259A). The guidelines were not

[17] Food and Drug Administration. Safer Technologies Program (STeP) for Medical Devices [Internet]. FDA.gov [cited August 2021]; Available from: https://www.fda.gov/medical-devices/how-study-and-market-your-device/safer-technologies-program-step-medical-devices

mandatory. NIST also referred to its Considerations for Managing Internet of Things Cybersecurity and Privacy Risks for additional guidance.

In 8259A, NIST recommended a baseline for cybersecurity on IoT, categorizing the baseline into the following categorical approach listed below:

- Device Identification – the ability to identify a device identifier to support asset and vulnerability management;
- Device configuration – the ability to address threats, privacy, or usability;
- Data protection – the ability to install cryptographic modifiers to render data inaccessible from unauthorized parties;
- Logical access interfaces – the ability to disable unnecessary access or restrict access as appropriate;
- Software update – the ability to update device software remotely and verify/authenticate updates prior to installation, roll-back updates to a prior version, restrict updates to authorized parties, and enable or disable updating.[18]

IoT Cybersecurity Act

In December of 2020, Congress signed the IoT Cybersecurity Improvement Act into law. (IoT Act). Pursuant to the IoT Act, federal agencies were required to adopt and update minimum information security standards. The intent was to ensure a set of standards for a crucial, yet vulnerable, part of our tech infrastructure.

In part, the IoT Act required NIST and the office of management and budget to take specified steps to increase cybersecurity for IOT devices, including requiring NIST to develop and publish standards and guidelines for the federal government to follow and use in management of IoT devices owned or controlled by agencies.

While the IoT Act is not binding upon private entities, the directives therein and the guidance forthcoming from NIST are instructive for private entities that manufacture or own/control wearable devices, for two reasons: (i) enhanced presentation to end users for delivery of secure wearable devices and (ii) a proactive step to design a level of compliance that anticipates further legislative activity on IoT devices.

In December 2020, NIST issued its draft IoT Device Cybersecurity Guidance for the Federal Government (800-213). The draft guidelines were issued as part of a series – the remaining documents were NISTIR 8259B: IoT Non-technical and Supporting Capability Core Baseline, NISTIR 8259C: Creating a Profile of the IoT Core Baseline and Non-Technical Baseline, and ISTIR 8259D: Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government.

In 800-213, NIST posed questions to federal agencies that are instructive for private enterprise manufacturing or distributing wearable devices, as listed below:

- What is the benefit of the IOT device and how will it be utilized?;
- What data is collected through or by the IOT device?;
- In what technologies will the data be stored?;
- With whom will the data be shared?;

[18] M. Fagan et al. IoT Device Cybersecurity Capability Core Baseline [Internet]. NIST. 2020 [cited August 2021]; Available from: https://www.nist.gov/publications/iot-device-cybersecurity-capability-core-baseline

- Will the device interfere with other aspects of operations or system functionality?;
- Would the device introduce unacceptable risks to the agency or result in non-compliance with cybersecurity requirements?;
- Does the device have known security or privacy vulnerabilities?.

NIST also recommended that Federal agencies adopt and implement these guidelines according to use context and other pertinent considerations.[19]

V. Emerging Environment and Guiding Principles

The private sector can play a material role in motivating manufacturers and distributors of wearable devices to move on improving cybersecurity of the devices. Purchasers of devices can implement their criteria in selection in accordance with strategic principles that incorporate some or all of the foregoing.

Thus, purchasers could implement a set of guiding principles in making their decisions and assess a potential vendor according to its presentation on these principles. Purchasers could query potential vendors on the principles identified by the purchaser, to facilitate selective criteria. In doing so, purchasers could reference NIST's recently released draft publication Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. (800-160, Volume 2). The guideline focuses on principles, concepts, and practices for engineering secure systems to create cyber resiliency. The draft guideline provides a description of a framework for cyber resiliency engineering and suggests that a cyber resilient system should be designed to achieve some or all of fourteen techniques, including the following:

- Adaptive response – an agile system designed to manage risks;
- Analytic monitoring – analysis of properties and behaviors of a system on an ongoing and coordinated basis;
- Contextual awareness – maintenance of a current representation of the enterprises' posture considering threats and resulting courses of action;
- Deception – design of procedures to mislead or confuse, or hide valuable assets from, an adversary;
- Privilege restriction – restriction of privileges for users that is consistent with system elements; and
- Realignment – design of the system to align with business function needs, reduce risks, and accommodate evolution from technical, operational, and threat environments.

The draft guideline also provides considerations for determining which cyber resiliency constructs are most pertinent to an enterprises' system.

Thus, purchasers could fashion their principles for selecting vendors according to vendors' display of adherence or adoption of the guidelines expressed by NIST in the draft guideline or in a resulting final guideline. These principles could include the following, flexible to the needs and structure of the market purpose for the device:

- The vendor's internal policy for addressing standards set forth by NIST or by a market trade group that addresses the concerns underlying the NIST standards;
- The vendor's internal development procedures for dynamically updating its standards on manufacture of the devices;

[19] National Institute of Standards and Technology. NISTIR 8259B (Draft). IoT Non-Technical Supporting Capability Core Baseline.2020[cited August 2021]; Available from: https://csrc.nist.gov/publications/detail/nistir/8259b/draft.

- The vendor's market resiliency for identifying challenges to its ability to continue operations in the face of threats in cyber, climate, market, or other vectors;
- The vendor's achievement on certifications or other quality metrics issued by a trade group for the vendor's market slot or "seal or approval";
- The vendor's willingness and ability to demonstrate capacity to meet standards that the purchaser presents to the vendor, similar to a capability maturity model.

VI. Conclusion

Wearable healthcare devices is a growing consumer segment that straddles the Internet of Things, smart devices, and medical devices. While wearable healthcare devices offer consumers the ability to be an active participant in managing their health, challenges exist in the technology. Devices may include vulnerabilities that allow the device to be compromised and expose personal data. Manufacturers may aggregate data across their consumer population and may not apply appropriate measures in limiting the types of data, amount of data, or data usage that consumers may assume are in place. This paper looks to concepts and guidance offered in safeguarding other types of technology as a foundation by which appropriate measures may be applied for consumer healthcare technology.

Appendix A: Additional Reading

For more information on wearable device security and privacy, check out the following links:

- https://www.wearabletechnology-news.com/categories/security/
- https://md2k.org/about/news/23-wearable-devices-security-usability-important.html
- https://zeguro.com/blog/new-security-risks-posed-by-wearables-iot
- https://usa.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store
- https://www.micromd.com/blogmd/hipaa-compliance-of-wearable-technology/
- https://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/
- https://www.webroot.com/blog/2019/01/23/smart-wearables-convenience-at-the-cost-of-security/
- https://us.norton.com/internetsecurity-iot-how-to-protect-your-connected-wearables.html
- https://ijisrt.com/assets/upload/files/IJISRT20DEC242.pdf
- https://ontech.com/mobile-security-checklist/
- https://www.verizon.com/articles/mobile-device-security/
- https://flex.flinders.edu.au/file/c81182bb-2896-48da-95b8-bb943d3f7722/1/Privacy%20and%20Security%20Issues%20of%20Wearables%20in%20Healthcare.pdf
- https://edge.siriuscom.com/security/mobile-device-security-in-the-workplace-5-key-risks-and-a-surprising-challenge
- https://cismobile.com/mobile-device-security-the-challenges-of-consumer-plus/
- https://www.vmware.com/topics/glossary/content/mobile-device-security
- https://www.securitymetrics.com/content/securitymetrics/us/en/mobile.html
- https://www.helpnetsecurity.com/2020/08/21/know-the-threats-to-mobile-security/
- https://www.condley.com/accounting-edge/wearable-technology-cyber-security-threat/
- https://infosecawareness.in/concept/security-awareness-on-wearable-gadgets
- https://www.twice.com/blog/executive-insight/executive-insight-wearables-and-data-privacy-what-consumers-need-to-know
- https://healthinformatics.uic.edu/blog/ethics-of-wearables/
- https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf
- https://www.healthline.com/health-news/consumers-concerned-about-privacy-personal-health-data-wearables-mobile-apps-072815
- https://www.coursera.org/lecture/iot-cyber-security/consumer-wearables-and-the-organizational-risks-gBoDr
- https://healthitsecurity.com/news/consumer-adoption-of-health-tech-slowed-by-privacy-security-concerns
- https://www.consumerreports.org/cro/magazine/2013/06/keep-your-phone-safe/index.htm
- https://www.healthcareinfosecurity.com/interviews/wearable-devices-security-risks-i-2764
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5905955/

- https://www.travelers.com/resources/business-industries/technology/how-companies-can-help-reduce-risk-from-wearables
- https://flex.flinders.edu.au/file/c81182bb-2896-48da-95b8-bb943d3f7722/1/Privacy%20and%20Security%20Issues%20of%20Wearables%20in%20Healthcare.pdf
- https://repository.gheli.harvard.edu/repository/collection/resource-pack-big-data-and-health/resource/11888
- https://www.sciencedirect.com/science/article/pii/S2352864817302985
- https://www.identityforce.com/blog/15-mobile-device-security-tips
- https://www.csoonline.com/article/3186164/10-security-risks-of-wearables.html
- https://iapp.org/news/a/wearables-where-do-they-fall-within-the-regulatory-landscape/
- https://searchsecurity.techtarget.com/answer/Wearables-security-Do-enterprises-need-a-separate-WYOD-policy
- https://www.wearabletechnology-news.com/news/2016/nov/15/wearables-are-secure-enough-enterprise-only-right-policies-place/
- https://informationsecurity.iu.edu/personal-preparedness/hardware-software/wearable-tech.html
- https://flex.flinders.edu.au/file/c81182bb-2896-48da-95b8-bb943d3f7722/1/Privacy%20and%20Security%20Issues%20of%20Wearables%20in%20Healthcare.pdf
- https://www.insideprivacy.com/data-privacy/legislation-seeks-to-regulate-privacy-and-security-of-wearables-and-genetic-testing-kits/
- https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2015-16/november-december/IoT-Big-Data-Consumer-Wearables-Data-Privacy-Security/
- https://blog.healthverity.com/ccpa-connected-devices-and-new-privacy-regulations
- https://healthtechmagazine.net/article/2020/09/3-reasons-why-wearables-bring-new-complications-hipaa-compliance