Privacy and Security Issues of Wearables in Healthcare

Keyur Tapan Shah
FAN - Shah0211
Student ID – 2160530

Supervisor: Prof. Trish Williams

June 2019

Submitted to the College of Science and Engineering in partial fulfilment of the requirements for the degree of Master of Science at Flinders University – Adelaide Australia.

DECLARATION

I certify that this work does not incorporate without acknowledgment any material previously submitted for a degree or diploma in any university; and that to the best of my knowledge and belief it does not contain any material previously published or written by another person except where due reference is made in the text.

K. T. Shah

Signature

Date: 14-06-2019

ACKNOWLEDGEMENT

The Master thesis is the most important part of the master's study. I also choose to do an 18-unit master thesis after consulting with senior students and teachers. I would like to convey my special thanks to my senior friend Amarjot Kaur who advised me to do my thesis under Professor Trish Williams.

Professor Trish Williams is the key person for me as supervisor towards successful completion of the Master Thesis. I appreciate her invaluable advice and timely feedback to successfully finish my Master Thesis.

ABSTRACT

The wearable industry is booming nowadays. Wearable devices once used as a fashion accessory, are now an important tool used in healthcare industries. Wearable devices like smartwatches, smart bands, fitness tracking, smart textiles and smart accessories are used in healthcare industries. This means a patient can monitor their health from home. With this huge advance in technology, there are privacy and security issues with wearable devices. This document presents the literature review of the wearable devices, and the use of it in healthcare. It examines the problems of wearables and the legislation and regulation of wearable devices in Australia, USA, and Europe. There are standards, guidelines, and regulations for privacy and security of wearable devices. These regulations and standards are not strict and many of the manufacturers do not follow the regulations. The user themselves contribute to the leakage data privacy and device security, as they are not aware of different threats and vulnerability of the devices. There should be strict rules and regulation for the wearable devices to maintain privacy, security and data stored in the device. This document also explains how the data can be attacked. Finally, it examines guidelines for consumers and recommendations for manufacture development, so a device is not attacked and thus protected. So, it follows, that if there are strong regulations and consumer awareness of different threats, the device and data stored in the device will be safe.

CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

ACRONYMS

IOT - Internet of Thing

NFC - Near Field Communication

GUI - Graphical User Interface

WHMS - Wearable health-monitoring system

Wi-Fi - Wireless Fidelity

HIT - Health Information Technology

DoS - Denial of Services

HIPAA - Health Insurance Portability and Accountability Act

WSN - Wireless Sensor Network

FDA - Food and Drug Autoimmunisation

ISO - International Organization for Standardization

TGA - Therapeutic Goods Administration

INTRODUCTION

In recent years, the electronic technology industry has made a huge investment in wearable devices. The companies are making different types of wearables like smart watches, fitness trackers, smart clothes, wrist bands, etc (Swan, 2012). The use of these wearables is being adopted for research and for our healthcare, like sleeping habits, checking our heart rate, the number of steps taken, running speed, etc (Garcia-Mancilla & Gonzalez, 2015; Sano & Picard, 2013).

We are entering a new computer era that is called Internet of Thing (IOT) (Siboni, Shabtai, Tippenhauer, Lee, & Elovici). The IoT is a keyword in which all the smart objects are contacted through internet. The IoT contains smart technology and machinery to communicate with other machines or objects. With this, a huge amount of data is being produced. This huge amount of data is being processed into use actions that can communicate and control things which make our life easier and safer (Karimi, Atkinson, & ARM, 2013).

Wearable technology uses these devices to monitor our health. Wearable devices are useful tools for encouraging and motivating users who use these devices to measure their fitness levels and healthcare. These can be a good way for delivering health related data and self-knowledge (Cafazzo, Casselman, Hamming, Katzman, & Palmert, 2012; Li, Dey, & Forlizzi, 2010).

The data collected by a device can range from heart rate, sleeping habits, temperature and location of the wearer. As such, privacy and security issues arise. So this becomes a prime device to target sensitive information (Arias, Wurm, Hoang, & Jin, 2015a). Privacy consent and security are the biggest problem in this field. There are few regulations and legislation for wearables in healthcare that protect the data and devices.

There are regulations and legislation in different countries, but every country has different regulations concerning wearable devices. These are explained in this document. Lastly this document has recommendations for manufactured devices and guidelines for consumer data and device safety.

The wearable devices stored large amount of health data which can be access by manufactures or third party without user knowing it. This creates huge privacy and security problem and the personal health data can fall into wrong hands. A user should be informed about the risk involved in it.

Significance of the study

This research is aimed to give knowledge about privacy and security of wearables which are used in healthcare. The objective is to review wearable devices that monitor our personal health in our day to day life and how to protect the devices.

The main impact will be on the developer and user of the wearable devices.

- It will provide help to understand why an individual should try to protect their own personal information.
- Manufacturers will understand the need for privacy and security and add some more feature in the devices.

Purpose of the study

There are many wireless techniques which are used to transfer data from wearable devices to mobile, cloud or a given destination. The wireless technology such as Bluetooth, Wi-Fi, near field communication (NFC) and infrared data association, are a few common ways to transfer data from a wearable to a given destination (Kim & Lim, 2015). However, there are many problems in transferring data through wireless. The transfer of wearable device data is usually without any encryption and much of the data that is stored on the device is not encrypted (Lemos, 2016).

Aim of the project

Wearable devices collect health data, living habits and the location of the wearer. As such, privacy and security issues arise. The device stores personal information of the wearer, so it becomes a prime target for an attacker who is looking to obtain the data (Arias, Wurm, Hoang, & Jin, 2015b). The main aim is to understand the privacy and security issues of wearable device, and the privacy of the data and identify the techniques and methods for managing security and privacy problems in wearable devices.

Research questions

Understanding the privacy and security issues of wearable devices, is the objective of this research. The research question is “how can data collected using wearable devices be protected to avoid misuse?”

LITERATURE REVIEW

The literature review explains the different aspects of wearable devices. There are many types of wearable devices in the market which are used to monitor our health. These devices are in the form of accessories, clothing and patches. These devices help to monitor our health at home and it also can help to diagnose different diseases and symptoms in our body. These wearable devices have also become a fashion style nowadays. These devices have different types of sensors which collects data from the surroundings. The wearable devices are growing in the field of healthcare, as they give real time feedback to the user or doctor. The wearable devices lack security, like password protection and encryption. Security in the wearable device is important because it contains sensitive health data of a user. The wearable devices have different types of security risks relating to cloud, hardware, software, sensor and many more which have been expanded on below.

What is a wearable?

Wearable is a thing which we can wear on our body. This type of technology has become a common part of world technology (Wright & Keith, 2014). The word wearable is often used with technology (wearable technology) and devices (wearable devices). The wearable technology should be mobile and means that it should go where the wearer goes (Billinghurst & Starner, 1999). Wearable technology and wearable devices are the words which describe computer and electronics that are integrated into our accessories and clothing which can be worn comfortably on the body (Sultan, 2015).

Types of wearables

Many large technology companies have entered into the market with wearable devices. These companies have expanded this technology into health industries. This technology is embedded in textile or accessories. These devices record different types of our living habits and help to motivate the user to live a better life (Patel, Asch, & Volpp, 2015). There are few wearables devices which are used to monitor our health, which are mentioned in Table1 and categorised into Accessories, Smart Cloths, Patches and Medical Devices.

Name	Types	Overview	Features	Cost
Accessories	Smart watch (Samsung gear, Apple watch, Fitbit)	A light weight and small wearable product on the wrist. It is also called mini computes which has functions. It is the latest evolution in the field of information technology (Chuah et al., 2016).	The user can measure their daily status. It monitors their heart rate, stress level, exercise, calories, sleeping habits and water intake level. The smartwatch also counts the distance and records the number of steps taken(Shah, 2018).	$100 - 2000
	Smart Shoes (Nike, Under Armour)	Smart wearable footwear which has different sensors inside the shoes (Kraft, 2018).	The shoes, tracks, analyses and stores running matrix. The shoes also detects landing, jumping, on which foot or which area of the foot. It can also tell stride length, speed, distance amount of ground contact time and cadence.	$250 - $450
	Smart glass	Immediate assistance for almost anything you want to do without a sighted person (Aira, 2018).	One tap of a button instantly connects you with a sighted professional agent who delivers visual assistance anytime and anywhere. The blind person can confidently navigate roads and city. Call the agent by the tap on the glass. Glass has camera on it, so an agent can see what is around the blind person and guide the person (Aira, 2018).	
	Pants	Wearable shorts - may understand muscles behaviour (Sawh, 2017).	The pants read and understands the muscles. It records the steps, distance, pace, time, length, motion profile, shocks and summery (Sawh, 2017).	$450-700

Name	Types	Overview	Features	Cost
Smart clothes	iTBra	Small and thin patch to wear inside the bra (Yan, 2019).	Wearable, comfortable intelligent to detect breast cancer. It identifies and categorize abnormal circadian patterns in otherwise healthy breast tissue (Yan, 2019).	N/A
	Smart shirt (Hexoskin)	The garment that helps to track our health condition and monitor our sleep (Draper, 2018a).	The smart shirt monitors heartbeat, ECG HRV (allowing stress monitor, fatigue assessment, load and effort) QRS and heart rate recovery, Breathing ratio and minute ventilation. It also counts steps and distance, positions peak and sleep tracker (Draper, 2018a).	$600
	Smart socks (Owlet, Sensoria Smart Socks)	It is the way to get real time update of the baby (Owlet) (Turner, 2017).	Smart Sock tracks heart rate and oxygen levels and notifies you in real-time if something appears to be wrong. It tracks all the basic metrics you'd expect, plus a few extra ones, including distance, speed, steps, calories burned, cadence, altitude, ascent, descent, heart rate (when wearing a connected heart rate monitor), foot landing, and foot contact, A virtual coach gives you feedback (Turner, 2017).	$400 - $600
Patches	Kenzen, TempTraq	A small layer of material which can be worn as accessories (Shreyas, 2019).	Measure body temperature, measures your heart and breathe to track your stress levels in real-time call heart rate variability (HRV) and ECG. Few also do sweat analysis (Shreyas, 2019).	N/A
Medical devices	Current Health Artificial Intelligence	A device worn on upper arms to calculate different health data.	Doctor can get real time feedback of the patients' health and monitor the patient health like ICU (Taylor, 2019).	N/A

Table 1 – Different Type of Wearable Devices

Data

Wearables have different types of sensors embedded in them, which collect the data from our body and transfer to a given place. There are two ways to transfer the data. One is proprietary and the other is third party. The propriety system is created by the device manufacturer. It can be in the form of a smart phone, computer, apps or cloud services. Whereas third party is developed and maintained by external devices to perform the specific functions (de Arriba-Pérez, Caeiro-Rodríguez, & Santos-Gago, 2016).

The wearable devices are currently used by the consumers to track the information that has been transferred through body sensors which includes heart rate and pedometer. This device has different software applications installed in it. They communicate information from the body and environment through sensors and deliver it to the consumers. It captures the body and environmental information of the consumers through sensors and stores it in the data storage box as developed in the smart phones (de Arriba-Pérez et al., 2016).

Ultrasonic waves are emitted from the human body (bones and skin). Smart devices are not connected with any internet or Bluetooth, it stores data in the device. When the devices are connected with the internet or Bluetooth it will transfer the data to the phone or given location (Årsand, Muzny, Bradway, Muzik, & Hartvigsen, 2015).

Wearable devices have sensors in them. The human body gives the ultrasonic wave, sensors catches those waves and calculate the data. This data is then transferred to the mobile or to a storage place through Wi-Fi or Bluetooth. (Kim & Lim, 2015).

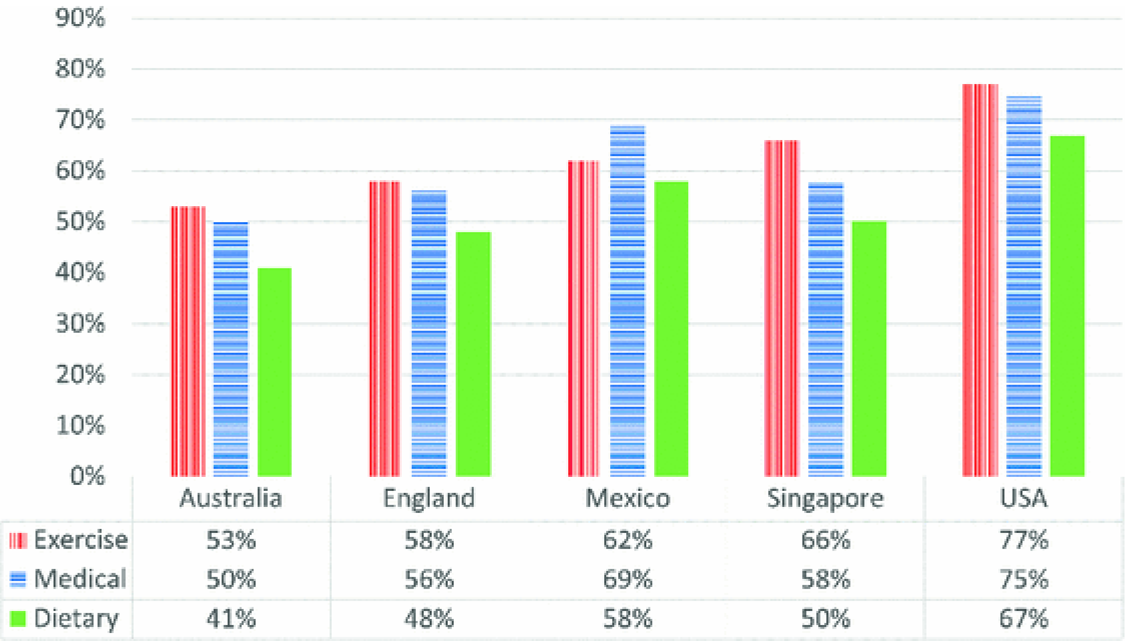
Use of wearable devices

The wearable devices and wearable technology have been the major growth area of technology in recent years (Sultan, 2015). Many companies have started to evolve more types of devices. They are smaller in size and have different sensor technology that can collect different information about their surroundings. The new wearable products are more sophisticated and can perform a wide variety of functions. However, new wearable products are not developed and produced by traditional wearable devices companies, but are made by computer and software companies. The wearable products became popular because it is easy to use, it can be used as a fashion style. The interface design of most wearable devices has GUIs, which is easy to use and interact with (Ross, 2001). Wearable devices are used for tracking and controlling our health and spearing healthy competition which gives real-time feedback. These devices are helpful for disabled people (Techopedia.com, 2018).

Use in healthcare

To use wearable technology is cheaper, as healthcare cost is increasing and world population has been ageing, so we need a device which could work in our personal environment. For this, different types of prototype and commercial products have been produced in the last few years, which aim to give real time feedback to the user, the doctor, and medical centre. This will indicate any health threat (Pantelopoulos & Bourbakis, 2010). Wearable health-monitoring systems (WHMS) have a lot of attention by researchers and industry during the last few years, as is shown by increasing corresponding research and development efforts (Gatzoulis & Iakovidis, 2007; Lmberis & Dittmar, 2007; Tröster, 2005).

Previously the use of this wearable technology was in the field of military and defence and has since shown to have had substantial benefit in healthcare. Nowadays, the wearables are mainly growing in the fields of health, fitness and dietary. Considering this demand, we can see from Figure 1 that the wearable is more popular in the medical field compared to other fields. (Saa, Moscoso-Zea, & Lujan-Mora, 2018).



	Australia	England	Mexico	Singapore	USA
🟥 Exercise	53%	58%	62%	66%	77%
🟦 Medical	50%	56%	69%	58%	75%
🟩 Dietary	41%	48%	58%	50%	67%

Figure 1 - Use of Wearables in Different Countries (Saa et al., 2018)

Advancement of technology and sensors brings new models for healthcare and wellness or disease management tools, which in turn improves the quality of life, particularly the aged by living at home longer. The sensor can be put in jewellery, clothes and other accessories. This is useful in managing our health in daily life and in real time (Korhonen, Parkka, & Van Gils, 2003).

Wearable devices for health monitoring have many types of sensors in the devices or implanted in them. These biosensors are capable of measuring significant physiological parameters like body and skin temperature, heart rate, oxygen saturation, blood pressure electrocardiogram and respiration rate, etc. The devices communicate via wire or wireless. The wearable medical system may have a wide range of components like wearable materials, sensors, smart textile, power supply, actuators, communication modules, CPU, interface for user, software and data extraction (Pantelopoulos & Bourbakis, 2010).

Data privacy and security

Wearables have many functions and many types of processes involved within them, like processing, data collecting storage and data transfer, however, with these wearable devices there are privacy and security issues (Lee Linda, Egelman Serge, Lee Joong Hwa, & David, 2015). These devices are worn on our body and are operated continually to take data from the surrounding, so they can be seen early and accessible to attackers. In this section we will discuss some privacy and security issues of wearable devices (Siboni et al., 2016).

What are the problems?

The wearables have rapidly gained the attention of consumers, is growing fast and will grow faster in future. But with this there are many problems in the devices (Eadicicco, 2015). The wearable devices are smaller in size, so therefore they have smaller battery sizes that need to be constantly charged (Eadicicco, 2015). The data stored in wearable devices are not encrypted. These devices often do not have any password protection, pin or biometric security and there is no proper authentication to access the data. If the devices fall into the wrong hands, there is a high risk that sensitive data can be leaked or it can risk a life threatening situation to the user (Sorber et al., 2012).

Wearable devices tend to connect to smart phones or other smart devices by Bluetooth, WI-Fi or NFC and this creates another entry point into the device. Our smart phone is connected with a device such as Bluetooth, but we do not know what else it can be contact with. This device has insufficient wireless security against the brute-force attack. The data is not encrypted, it is stored and sent to other devices. The data is not secure when it is stored on a manufactures server or cloud service. Third party apps do not have a security standard and may steal the data which is not encrypted (Liu & Sun, 2016).

The wearable devices have their own operating system and application. They have become more common and so they are also being targeted. There is a need to apply the same principle as apply to laptops, desktops, mobile etc. These devices should be fully patched and up-to-date to avoid the vulnerabilities of the wearables (Siboni et al., 2016).

The main problem is energy constraints. The IoT devices need lots of battery power and devices are using low-power CPUs having low clock rates. So, computationally cryptographic algorithms which need more power, cannot be ported into a low powered device. Another consideration is, memory constraint IoT devices are built with limited RAM and flash memory compared to the traditional digital system regular security algorithms and are not designed specifically considering the memory efficiency, because the traditional digital system uses spacious RAM and hard drive. These security schemes may not have enough space, after booting up the system software and operating system. So, normal security algorithms cannot be used for securing IoT devices. Tamper resistant packaging- IoT devices may be developed in a remote area and left there unattended. An attacker might tamper with IoT devices. The attacker can extract the cryptographic secrets, modify the program or replace it with malicious nodes. IoT OS, which are embedded with the IoT devices, have thin network protocol stacks and may not have enough security modules. So, the security module designed for the protocol stack should not be thin, it should be strong and tolerant. Installing a security patch on the IoT devices and mitigating the potential vulnerabilities is not an easy task. Remote reprogramming might not be possible for the IoT devices, as the operating system or protocol stack might not have the ability of receiving and integrating new code or library. The secrecy and confidentiality of the on-air and stored information should be strictly preserved. It should to limit the information access and disclosure to the authorized IoT node, and preventing access by or disclosure to unauthorized ones. It should not give or read the data from other close devices, as this can be a security problem (Hossain, Fotouhi, & Hasan, 2015).

Healthcare is one area in which we can use wearable technology to monitor our health daily. The healthcare cost is increasing, and the world is ageing, there is a need to monitor our health while we are not in hospital but in our personal environment. To address this, many new prototype systems and products are being produced in recent years. This new type of technology aims to give feedback in real time about our health condition. It can be useful to the user or for supervising medical care by a personal physician. This helps patients to know their health status and it will help to identify threatening health conditions which have arisen or will arise in future. Most of the wearable technology was developed in 2010 which focused on fitness. In future wearable devices are expected to perform many tasks and it may become an important part of our life. As such, the issue of privacy and security will be important. Security is the main aspect of the system (Gatzoulis & Iakovidis, 2007).

Wearable products in healthcare should not be treated as an application of emerging technology in healthcare but should be regarded as a high privacy consent product. Like other types of data and information, personal health data is more sensitive for individuals. So considering the privacy factor on customers' acceptance of healthcare, wearable product are necessary (Bansal & Gefen, 2010). HIT (Health Information Technology) may aggravate individual privacy concerns over misuse of personal health data. When user perception of benefits exceeds the privacy risk, the user would choose to adopt healthcare wearable technology, otherwise the technology will not be accepted (Li Han, Gupta Ashish, Zhang Jie, & Rathindra, 2014). Adopting healthcare wearable technology would involve a highly important privacy risk, in which the user may face the balance between perceived benefit and perceived privacy risk. The benefit of adopting wearable devices has been measured by perceived expectation, relating to motivation (Xu, Dinev, Smith, & Hart, 2011). The wearable devices which are used in healthcare, are mostly wireless in nature. This can have various threats to the system. These attacks and threats can cause serious problems to an individual who is using the wireless system. The attacker can track the location of the person. People with malicious aims may use private data to harm the person (Al-Ameen Moshaddique, Liu Jingwei, & Kyungsup, 2012).

Risk

The survey about IoT has shown that privacy and security are the main problem and we need to solve this problem before we adopt these wearable IoT devices (Atzori, Iera, & Morabito, 2010).

Device Architecture

The architecture includes hardware and software which includes security considerations. These wearable devices have low powered memory size, power, computation capability and low bandwidth communication (Hiremath, Yang, & Mankodiya, 2014). This results in security problems, as only lightweight encryption methods are applied in order to encrypt stored data and transmit data through the devices (Al-Muhtadi, Mickunas, & Campbell, 2001; Shrestha & Saxena, 2018).

On the software side, the operating system of the wearable devices is highly visible to zero day vulnerabilities (Hiremath et al., 2014). The wearables devices are cheaper than the smart phone and PC, so they are less updated by the manufacturers (Clayton Locke, 2014).

Network Connectivity

Wearable devices are constantly connected to internet through Wi-Fi, mobile internet or indirectly through Bluetooth. The wearable IOT devices are not designed with security in mind due to low resources and cost cutting (Cooper, 2015) mentioned in (Siboni et al., 2016). However, due to light authentication programming in the wearable, it is possible to manipulate and control the devices at the weakest point, when data is sent or received.

Our wearables are connected to cloud apps and enterprise network systems, this can be the starting point for an attack. It means that malware or different forms of attack can be a possible path that a hacker can get early access to corporate networks and steal the data or create a ransom for sensitive data (J. A. Martin, 2017a).

The Bluetooth technology has many advantages which communicate with personal devices, but this technology has many threats, vulnerabilities and risk. Today Bluetooth faces some problems like denial of services (DOS), man-in-the-middle and data corruption in different types or ways. This type of attack is called bluesnarfing. Bluesnarfing allows the attacker to get access to Bluetooth enabled devices by exploiting a firmware. Bluesnarfing is started by an attacker sending an unprompted message to the Bluetooth enabled devices. The attacker then sends spam and a phishing message to a user who is connected. Bluebugging is one type of hacking technique. This type of attacker gets the access of the victim’s devices and allows the attacker to make a phone call, delete contacts or listen to owner’s conversations. The DOS hacker sends a request to the victim, which causes battery degradation. Bluetooth also supports third party extension. If the devices do not have proper security or authentication to the network then the devices can be compromised (Bouhenguel, Mahgoub, & Ilyas, 2008a).

Collection of Data from Wearable Devices

The main concern for wearable devices is the type of data they collect, which leads to privacy and information theft (Lee Linda et al., 2015). The data is the most important asset, so many hackers collect data about customers and organizations, through vulnerable wearable devices Hammond cited in (Hammond cited in Siboni et al., 2016).

From a customer’s point of view, most data collected is personal and is sensitive data about a wearer’s habits, behaviour and also private health details (Hiremath et al., 2014; Swan, 2012). Nowadays wearables also have been used in the enterprise environment to increase business (Perera, Liu, & Jayawardena, 2015). The companies might exploit them to violate employees privacy, an employer can track employees actions and moreover see their health condition. So, the sensitive data might become accessible to outsiders and can be exposed to un-authorized people through these devices (Siboni et al., 2016).

As the technology has increased and we are adopting IOT, there is growing concern for security and safety in medical devices. A U.S department says that medical devices have been increasingly targeted by ransomware attacks. As per Mr Edwards the director of Department of Homeland Security’s Industrial Control Systems Cyber Emergency Response Team said that this is the time where computer malicious activities will affect medical devices (healthmanagement.org, 2017).

Cloud Computing

Wearables devices use the cloud computing to store information. The data is moved onto cloud which means that the wearer’s health data is being exposed to external threats which may break security rules, according to American regulation institute HIPAA. When data moves to the cloud, the sensitive data can be exposed and several external threats occur as the data can be accessed through the internet (Hussain et al., 2018).

Security Risks in Wireless Sensor Networks (WSN)

The security problem in healthcare with sensor networks, is a concern. Healthcare applications of sensor networks is simple compared to WSN applications, most of the security problems are similar. The threats are classified into two, passive and active. In passive the attacker can change the destination of packets or may change the routing. The attacker may also steal the health information by eavesdropping to wireless communication networks. Whereas, active threats are more dangerous than passive counter parts. Attackers can find the location of the wearers by eavesdropping. This can lead to a dangerous situation for the wearer (Kargl, Lawrence, Fischer, & Lim, 2008).

Authors also say that attacks in health monitoring devices are done by making changes in health data and eavesdropping. The attacks which can happen in healthcare systems with WSN is explained in Table 2.

Attacker Assumption	**The risk to WBAN**	**Security requirement**
Computation Capability	Data Modification	Data Internality
	Impersonation	Authentication
Listening Capability	Eavesdropping	Encryption
Broadcast Capability	Replaying	Freshness Protection

Table 2 - Security Risk to WBAN and Corresponding Security Requirement (Kargl et al., 2008)

Data Modification – Attackers can delete or edit some data and send some modified data to the receiver to activate some illegal purpose. The health information is crucial. This can result in a system failure or cause disaster to a wearer or both.

Impersonation – If a hacker eavesdrop a wireless sensor node, information, can be used to cheat other nodes. The data can be used for malicious activities.

Eavesdropping – Anyone can intercept radio communication between wirelesses nodes easily.

Replaying – The attacker can replace a piece of original information with eavesdrop information to achieve the same purpose.

Privacy is also among the major concerns of wireless sensor networks which are used in healthcare. Under the legislation, healthcare data is considered as private data. Privacy issues may arise in many ways. Data sent out form wireless networks can pose serious threats to an individual (Khan, Jabeur, Khan, & Mokhtar, 2012). If the issue with privacy is not resolved in a clear and open way, then there will be a risk in mistrust and the technology will not be useful for valuable applications where it gives significant advantage (Al-Ameen Moshaddique et al., 2012).

Normally there are few users of data, that is, doctors, nurses and technical staff. This limits the number of users in the system. Well defined regulation and guidelines should be adopted for use of data and user limits. But in case of emergency or remote monitoring, it may be necessary to disclose information to other people in order to attend the patient in need (Al-Ameen Moshaddique et al., 2012).

The malicious third party application can steal all the information from your wearable and sell to other organizations so that they could compromise consumer health risk. If a person is victim of this kind of data breach, then that person could face increasing health cover cost or policy cancellation (Draper, 2018b).

If the wearable device is left unattended, it can cause huge security problems. The device can be hacked easily. If the device is hacked, the attacker can access personal information and health data (Jhajharia, Pal, & Verma, 2014).

After reading we understand different problem with wearables devices. The main consent for wearable devices are privacy and security issues. There are different ways through which data can be leaked or hacked. The data stored in the device is personal data and sensitive health data of the user. With the help of that, an attacker can early track the habit and behaviour of a user and even the data stored in the device or external devices can be edited or stolen as it is not encrypted. A third party application can take the sensitive data from the device and sell to different organisations for money. Data transferred through Wi-Fi, Bluetooth or NFC can be easily hacked and read by an attacker. As days pass the security and privacy issues will become the main problem to solve.

METHODOLOGY

This section is about the research methodology which includes different tools and techniques used for data collection and understanding a case study. This section also lists different types of case studies of which one was selected.

Case Study

The method selected for this research is Case Study. This is being used to study a particular information systems case and to narrow down a broad field of research. The case study methodology is good to describe an ecosystem or testing the theories and models which actually work in real life. In case studies, the researcher analyses existing cases (Explorable.com, 2018).

The case study refers to a method analysis or specific research design for understanding the particular problem. It is an in-depth investigation of a single person, group, event or community. Typically, data is gathered from a variety of sources by using several different methods (Baxter & Jack, 2008).

Types of Case Study

Explanatory – Explanatory case study is used to explore phenomena. The explanatory case study should have a proper description of the case, alternative explanations and conclusions on the basis of explanations which contain facts (Harder, 2012).

Exploratory – The exploratory case study is used to explore the clear phenomena by having lack of initial research, which can have planned hypotheses, and/or there is limitation to select case study (Harder, 2012).

Descriptive – The descriptive case study is focused on details, in which theory and questions about phenomena are study at the output (Harder, 2012).

Multiple case studies – Multiple case studies, is known as collective case study. This involves substantial study of a number of case studies. The researcher chooses cases which are simpler in order to analyse the outcome from all cases. This is like having multiple experiments (Albert J. Mills, Durepos, & Wiebe, 2012).

Collective – Collective case studies are similar in nature and description to multiple case studies. In this, a number of case studies are studied together (Harder, 2012).

Intrinsic – The intrinsic case study is the study of a person, department, and enterprise where the case is the main interest of investigation (Grandy, 2012).

Instrumental – The instrumental case study is like an intrinsic case study but provides inside information into a specific issue, building theory or redoing the case (Grandy, 2012).

Methodology Selected

A case study method was selected to obtain rich and in depth information about the privacy and security issued in wearable devices used in healthcare. The regulations of the different countries was used to make this case study (Froggatt, 2011). This research needs to be seen from different aspects. The case study is the research methodology which has been selected to give the outcome of the thesis. There is different types of case study. Explanatory type of case study is selected to give data collection and guidelines for wearable devices and answers the research question. The figure 2 shows graphical steps involved in designing the case study.

This Explanatory method was selected because in this, wearable devices need to explore the regulations of the wearable devices in different countries. After studying this about wearables and the regulations, an alternative solution has been provided for the user in this document.
Research design – The coherent work flow module gives an over view of this document.

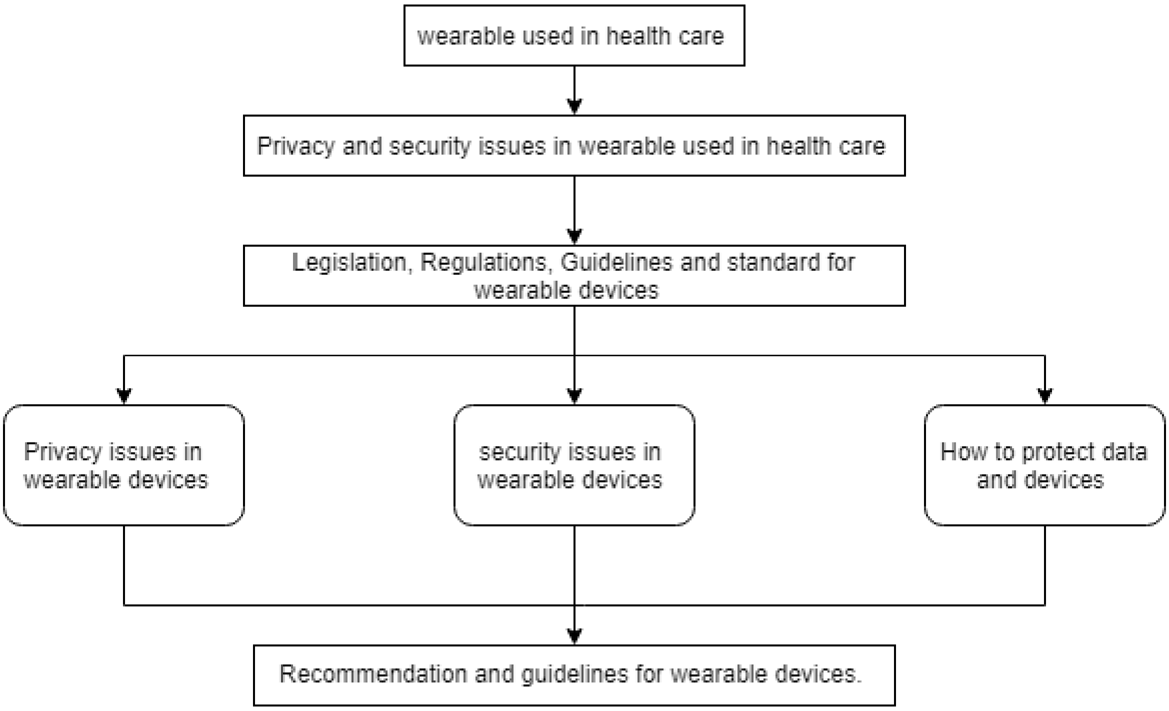

wearable used in health care
Privacy and security issues in wearable used in health care
Legislation, Regulations, Guidelines and standard for wearable devices
Privacy issues in wearable devices
security issues in wearable devices
How to protect data and devices
Recommendation and guidelines for wearable devices.

Figure 2 – Research design

Limitations of case study methodology

The case study methodology, is complex and the resulting case study can be difficult for the reader to understand. The case can be too lengthy, too detailed for people to read and understand. Sometimes the researcher is left with his own abilities and instinct to give the final output (Reis, 2009). The case study provides little basis for scientific generalisation, as it uses limited amounts of research and the study is done as a small part of work on this subject. It will not answer the question completely (Zainal, 2007). Many devices are not out in the market and are still in the developing phase, so cannot be studied.

RESULTS

Current solutions

There are several ways to check and reduce the privacy and security risks offered by wearable devices. Some of the ways are explained below.

- To reduce the chances of revealing personal information, the type and size of data stored on the device should be limited and protected by means of encryption (Tolentino, 2013).
- Application of automatic wipe features and data cleansing helps in deleting unnecessary data (Blum, 2015b).
- Application of Bring-Your-Own-Device (BYOD) privacy and security polices by companies by using encrypting measures to detect new connected devices and protecting sensitive information from eavesdropping and theft (Upton, 2015).
- Implementing the rule of least privilege can help keep a check on employees to read and write restricted data as well as protecting data from external threats (Blum, 2015a).
- Applying validation, clearance and liability measures for wearable devices connected to the network directly (Clayton Locke, 2014).
- Bluetooth connectivity of devices (Bluetooth-enabled devices) should be turned off whenever the device is not in use, reducing the risks of intrusion (Lloyd, 2014).
- Device software are to be kept updated by downloading and installing necessary updates and patches by the users (Siboni et al., 2016).

If in case the wearable devices fail to moderate the above mentioned security issues, with common mobile devices such as laptops, tablets, smartphones etc., then highly sensitive places will be needed to ban them. This would act as an infrastructure solution, so as to secure and protect the confidentiality and information of not just the wearer but also people in his/her surroundings (Brandon, 2014).

Additionally, privacy and security levels of wearable IoT devices should be regularly checked without affecting user’s privacy. This can be done by using selected security testbeds for wearable devices. This aims to (1) assess security levels of the devices, and (Molisch et al.) and (2) execution of security testing for devices affected by malicious threats. Unknown conditions for such attacks can be speculated for identification of context-based attacks (Siboni et al., 2016).

The social issues of wireless body area network (WBAN), includes privacy and security legal issues. The communication of the data between sensors and server over WBAN and internet should be encrypted to protect user's privacy. Legal regulations should be necessary to access sensitive data (Jovanov, Milenkovic, Otto, & De Groen, 2005).
The IOT enable a device to store the data in physical devices and cloud storage. Sensitive data and security credentials might be kept within IOT devices. So poor physical security level and data stored in cloud can be easily access by hacker.

The devices should be updated and patched regularly, and security measures applied so that the attacker should not be able to disclose the sensitive data that is part of the cryptographic software update configuration.

Legislation/ regulation

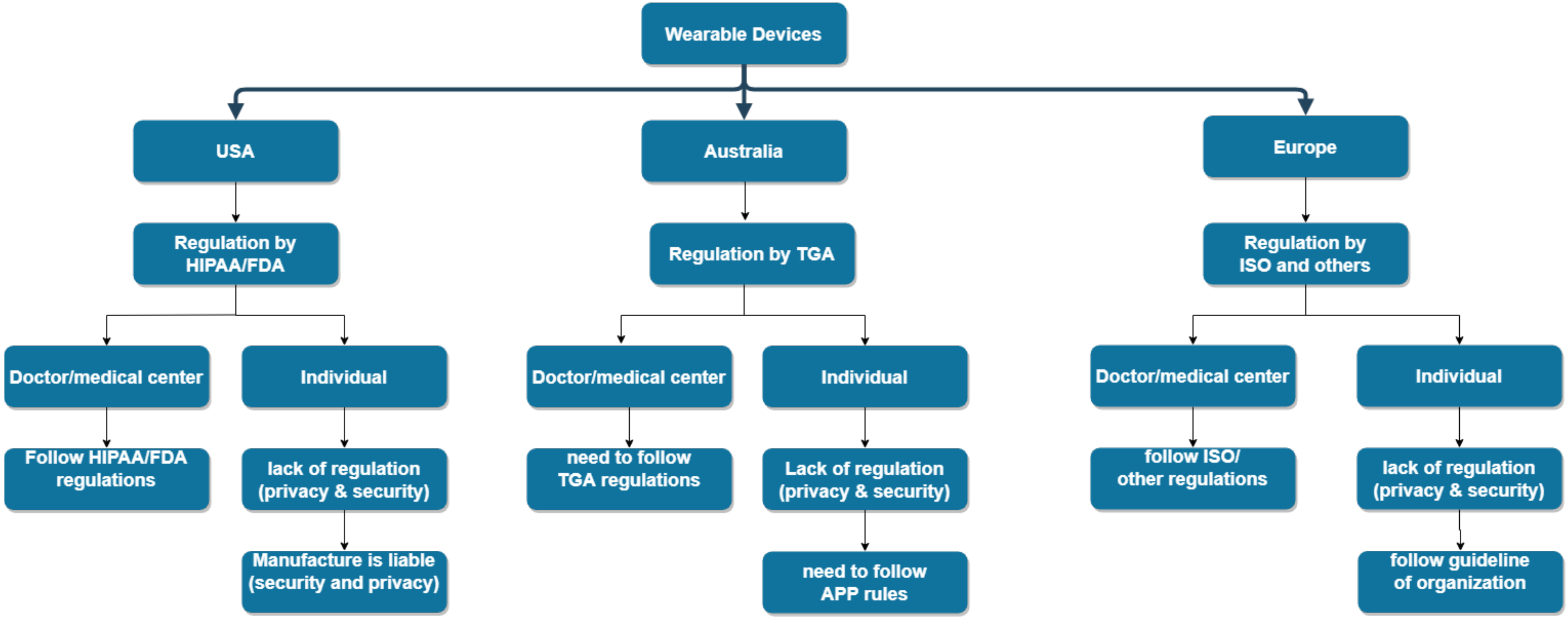

Wearable Devices
USA
Australia
Europe
Regulation by HIPAA/FDA
Regulation by TGA
Regulation by ISO and others
Doctor/medical center
Individual
Doctor/medical center
Individual
Doctor/medical center
Individual
Follow HIPAA/FDA regulations
lack of regulation (privacy & security)
need to follow TGA regulations
Lack of regulation (privacy & security)
follow ISO/ other regulations
lack of regulation (privacy & security)
Manufacture is liable (security and privacy)
need to follow APP rules
follow guideline of organization

Figure 3 – Regulations for Wearable Devices in the USA, Australia and Europe.

Figure 3 explains different regulations followed in different countries. When healthcare and doctors access the device to monitor the health, then it is same in all the three places but when an individual uses then it differs from place to place. This just gives an over view of different regulations in USA, Australia and Europe.

The wearable devices are established in the market, but we know that we need standards and regulation for needed functionality, privacy and security, to obtain maximum benefits for the wearer. There are many regulations and standardis in the market for wearable devices and IoT. With the support of industry and stakeholders, new standards and regulations can be made for the privacy and security of the wearer (Ash, 2016). The data collected from wearable devices is more personal and the manufacturers try to have a good balance between device, privacy and security of the devices. On one hand big companies are promoting their devices and encouraging people to wear them and on the other hand they are protecting their privacy and safety (Wellocracy, n.d.).There are few institutes which make regulations and standards for wearable devices which are used in healthcare, like HIPAA, FDA, ISO and TGA. In this section I have described the regulations by different institutes (Saa et al., 2018).

USA

HIPAA – Health Insurance Portability and Accountability Act

Legislation

HIPAA – Health Insurance Portability and Accountability Act (HIPAA) is part of HHS (Health & Human Service). It is the aim of this U.S department to protect the health and well-being of all Americans. This department focuses on advanced medicine, public health and social services.

Regulations

There is some uncertainty about, where HIPAA is responsible and where it is not for wearable devices. But one thing is clear that when medical devices or medical technology equipment is in use, the HIPAA regulations should be applied. This may include health plans, healthcare, healthcare providers that engage in certain payments and other financial transactions.(Snell, 2017)

When consumers wear the smart watch, HIPAA does not come into action. So when a user tracks the number of steps and heart rate monitoring it does not come under HIPAA regulations. Even the big companies like Fitbit, Samsung and Apple, devices are not HIPAA compliant. These big companies still work on devices which can be HIPAA compliance. General Manager of Fitbit said that they will launch a device which is fully HIPAA compliant and it will follow HIPAA regulations (Snell, 2017)

As a consumer, if I go to buy a wearable device, the data collected in that device is not bound under HIPAA, whereas if a doctor or hospital gives the wearable device to a client to collect healthcare data, that data is protected by HIPAA law (Lee, 2009).

The businesses are free to make their own rules for controlling information and data that falls outside the space of HIPAA (Roos, 2009). Many companies have their own private policies. Protected Health Information (Chuah et al.) Subject to the HIPAA rules, which stops disclosure of the PHI apart from a few circumstances. The Covered Entities cannot enforce the user to sign privacy rights. The company must obtain authorization from a user when they disclose information, users can revoke this at any time, and it should be presented to the user in a document about disclosing the information. The Covered Entity can remove personal identifier information from PHI before disclosing (Nina Kostyukovsky, 2018).

Guidelines

The HIPAA has seven security guidelines which cover Centres for Medicare and Medicaid services (CMS) on the "Security Standards for the Protection of Electronic Protection Health Information". Below are the sever guidelines for security rules.

- Security 101 for covered entities
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational, Policies and Procedures and Documentation Requirements
- Basics of Risk Analysis and Risk Management
- Security Standards: Implementation for the Small Provider (HHS, 2018).

FDA Food and Drug Administration

Food and Drug Administration is the oldest consumer protection agency in America, which is run by federal government. This agency looks after, food, drugs, medical devices, radiation emitting product, vaccines blood, biologic, veterinary, tobacco product and cosmetics (FDA, 2018c).

Manufacturers which make mobiles medical apps need to follow FDA regulation which are written below. It is divided in different classes.

"Class I devices: General Controls, including:

· Establishment registration, and Medical Device listing (21 CFR Part 807);

· Quality System (QS) regulation (21 CFR Part 820); ·
Labelling requirements (21 CFR Part 801);
· Medical Device Reporting (21 CFR Part 803);
· Premarket notification (21 CFR Part 807);
· Reporting Corrections and Removals (21 CFR Part 806); and
Investigational Device Exemption (Diez, Touceda, Camara, & Zeadally) requirements for clinical studies of investigational devices (21 CFR Part 812).

Class II devices: General Controls (as described for Class I), Special Controls, and (for most Class II devices) Premarket Notification.

Class III devices: General Controls (as described for Class I), and Premarket Approval (21 CFR Part 814) (FDA, 2015).

FDA has also classifications for almost 1700 different types of mobile devices which are grouped into 16 medical specifications. These classes need to be applied on devices for safety use for consumers.

“1. Class I General Controls

- With Exemptions
- Without Exemptions

2. Class II General Controls and Special Controls

- With Exemptions
- Without Exemptions

3. Class III General Controls and Premarket Approval (FDA, 2018a)”

If the product intends to be used for diagnosis, prevent, cure or mitigate the disease for human or animal, or affect the stature of animal or human, the product needs to be approved by FDA. This device is classified in three classes which are based on the risk of the user. Many devices also need premarket notification approval. If the product is in class III, premarket approval is required. If a company makes any changes to the product, then they have to resubmit it for re-approval. The big companies like Apple, Samsung and Fitbit do not like to do many changes as they have to resubmit approvals. So if we see the FDA approved stamp on products it means that it is safe to use (Sumra, 2018).

Guidelines

Technical Considerations for Additive Manufactured Medical Devices - Guidance for Industry, Food and Drug Administration

Software as a Medical Device (SAMD): Clinical Evaluation - Guidance for Industry and Food and Drug Administration Staff (FDA, 2018b).

Standards

- ISO/IEEE 11073 standards to wearable home health monitoring systems – This standard will outline communication between medical devices and external computer technology. It also describes automatic data capture of client and device operational data.
- IEEE 11073-10406-2011 - Health informatics--Personal health device communication Part – these standards describes the communication of personal health devices like ECG with cell phone and PC and personal health applications.
- Drivers privacy protection act of 1994 – This act is about privacy and disclosing personal information (Deborach Thoren-Peden & Meyer, 2018).

Australia

TGA - Therapeutic Goods Adminstration

Legislation

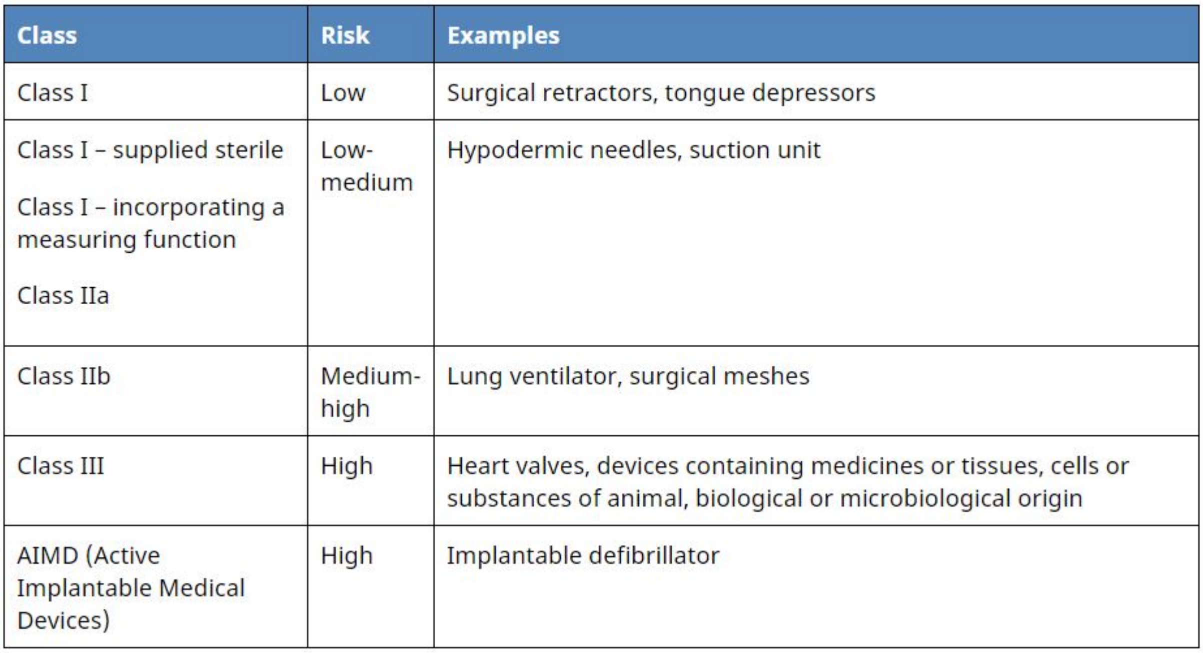
Therapeutic Goods Administration is a regulatory institute for therapeutic goods in Australia. This company regulates and orders the Therapeutic goods line advertising, product appearance, appeal guidelines and labelling.

Regulations

Wearables can be used for one or more of the following:

i. Prevention, monitoring, treatment or alleviation of disease;
ii. Diagnosis, alleviation of or compensation for an injury or disability;
iii. Investigation, replacement or modification of the anatomy of a physiological process;
iv. Control of disease (TGA, 2017a).

As per Australian privacy principal (APP), this act governs the rules and regulations about private data by the private or public sector. The APP says that the personal data which is collected by wearable devices should not be used for any other purpose, unless the customer permits or in a critical situation (Saa et al., 2018). It seems that Australia has some good regulations on protecting private data.



Class	Risk	Examples
Class I	Low	Surgical retractors, tongue depressors
Class I – supplied sterile Class I – incorporating a measuring function Class IIa	Low-medium	Hypodermic needles, suction unit
Class IIb	Medium-high	Lung ventilator, surgical meshes
Class III	High	Heart valves, devices containing medicines or tissues, cells or substances of animal, biological or microbiological origin
AIMD (Active Implantable Medical Devices)	High	Implantable defibrillator

Figure 4 - Shows How Medical Devices Are Classified By TGA (TGA, 2017b)

Guidelines

- Therapeutic Good (Medical Devices) Regulations 2002

Standards

- Data Privacy Act 1988- This act regulates the holding of personal information of individuals or sensitive information (Standards, 2016).
- IEC TC 62: Electrical equipment in medical practice – This standard describes electric equipment use and it includes, frameworks, data privacy and data integrity (Standards, 2016).
- Australian Privacy policy – This act describes handling personal information in any field like healthcare, business or Information Technology (Standards, 2016).

Europe

ISO and others

ISO stands for International Organization for Standardization. This is an international company that develops and publishes international standards for consumers and companies. ISO creates standards which has requirements, guidelines or characteristics to make sure that products are fit for that process (Ash, 2016). The smart wearables can be used as medical devices but only when a physician provides it and the patient agrees to wear it. In this case, healthcare is liable for the security and privacy of the devices. The data generated from wearables, may have a secondary use. The doctors need to approve who has access to the patient's data, whether it is used for research or not. The data transition, storage and processing should be fully secured. There are guidelines for the manufactures to follow, so there are less privacy and security problem with the wearable devices (Ruck & Limited, 2015).

Standards

- IEC/EN/UL 60601 (Medical devices) – this standard consist of safety of rules and regulations for medical equipment (Flynn, 2015)
- P360 - Standard for Wearable Consumer Electronic Devices – this overviews the architecture of the wearable devices and security of devices (de Arriba-Pérez et al., 2016).
- ISO/IEEE 11073 standards to wearable home health monitoring systems – this standard was for monitoring our health from home with wearables devices (Yao, Warren, & computing, 2005).
- IEEE 802.15.4 - Standard for Low-Rate Wireless Personal Area Networks – It talks about wireless communicate between the body and sensors in wearables devices (Molisch et al., 2004)
- IEEE-P1912 -Standard for Privacy and Security Architecture for Consumer Wireless Devices – This standard describes end used security, communication user authentication, sharing personal information and control of tracking items.
- IEEE P2413 Standard for an Architectural Framework for the Internet of Things (IoT) - It focuses on safety, privacy, security and protection of IoT devices.
- Dir 95/46/EC Data Protection – This standard describes data protection in European countries. How data should be processed and stored in wearable devices (Ruck, 2015).

Data collection

On the basis of the literature review, all the threats and vulnerabilities are mentioned below in Table 3, outlining threats and vulnerabilities. There are many types of threats and vulnerabilities through which our data and devices can fall victim in the wrong hands. People with a criminal mind can threaten vulnerable devices. The threats and vulnerabilities have been bifurcated on the bases of technical and non-technical. The description focuses on the use of wearable devices which are used in healthcare.

	Threats and vulnerabilities	**Technical or Non-Technical issues**	**Privacy and security**	**Outcomes**
1	GPRS	Technical	The GPRS helps to track our jogging pathway.	Data can be stolen while transferring data from different devices by eaves dropping, it allows the hacker to see the current or past location (Al-Ameen Moshaddique et al., 2012).
2	Bluetooth	Technical	The Bluetooth has low energy usage, so it is built with low security feature. The third-party Bluetooth receiver may be listening to information to capture sensitive information (Arias et al., 2015b).	Bluetooth is prone to vulnerabilities, in this the hacker can access the device and control the system and applications (Biggs, 2017). Data can be stolen while transferring data from different devices by eaves dropping (Al-Ameen Moshaddique et al., 2012)
2	Wi-Fi	Technical	Wi-Fi is used for communication through the Internet (Whitmore, Agarwal, & Da Xu, 2015)	Data can be stolen while transferring data from different devices by eaves dropping (Al-Ameen Moshaddique et al., 2012)
3	Data stored in device	Technical	Many devices do not use cryptography because of low powered devices (Fabietti et al., 1991).	The data stored on wearable devices and external devices are not encrypted, if the device has been hacked all the data can be seen by the hacker so, there is no confidentiality (Al-Ameen Moshaddique et al., 2012).
4	Theft	Non-Technical	Intentional impact	An attacker can see all the personal health data which is stored and can misuse that data which is stored in the device (Das, Wazid, et al., 2017).

5	Lost	Non-Technical	Unintentional impact	An attacker can see all the personal health data which is stored and that person can misuse that data which is stored in the device (Das, Wazid, et al., 2017).
6	Software or applications and operating system	Technical	The Software or applications attack happens due to Configuration change, and capturing data (Jiang et al., 2015).	Third party application can track the user's health data which leads to privacy breach (Ching & Singh, 2016).
7	Human error	Non-Technical	The device can be lost/theft, GPS, Wi-Fi, Bluetooth can be kept open and it can be unattended for a long time.	This can lead to leakage of information.
8	Cloud	Technical	Data stored on cloud is new technology to store and access data online (Urias, Van Leeuwen, Stout, & Lin, 2018).	Data stored in cloud are not secured, wearer health data is being exposed to external threats (J. Zhou, Cao, Dong, & Lin, 2015).
9	Tampering	Technical	The wireless technology is used to communicate between wearable which provides a chance for an attacker to tamper and read data (Das, Zeadally, Wazid, & Engineering, 2017).	The unauthorised access to the device, can extract the cryptographic secrets, modify a program or replace it with malicious nodes (Arias et al., 2015b).
10	Device policy	Non-Technical	The manufacturer should clearly maintain the use data in the policy. The User should also go through the device policy and should understand the signification of health data (T. Martin, Jovanov, & Raskovic, 2000).	Often manufacturer should clearly mansion about the use of hath data in their policy. The use of health data can be misused as per some policy (Das, Zeadally, et al., 2017).
11	Eavesdropping	Technical	Intercept radio communication between wirelesses nodes (Kargl et al., 2008).	The leakage of identifications allows unauthorised access to health data (Kargl et al., 2008)
12	Data is not encrypted	Technical	Many wearables do not have encryption as it needs more power (Haghi, Thurow, & Stoll, 2017).	When devices are being hacked or falls into the wrong hands , an attacker can see all the sensitive data which is

				stored in the devices as the data is not encrypted (Das, Zeadally, et al., 2017).
13	Unattended wearable device	Non-Technical	Device not been used due to the poor interest of user (Jhajharia et al., 2014).	The unattended devices can be early accessed and all the data can be retrieved. This results in leakage of sensitive data. (Jhajharia et al., 2014).
14	Use Authentication method	Technical	The manufacture only puts a minimal level of authentication or no authentication method in many devices (Mahalle, Anggorojati, Prasad, & Prasad, 2013).	The unattended device can be hacked easily. Anyone can track the data from wearable devices (Jhajharia et al., 2014).

Table 3 - Threats and Vulnerabilities.

The goal is to protect the privacy of a patients' health data while allowing users to adopt new wearable technology to improve the efficiency of the technology. The Wearable devices store large amounts of personal health information which can be accessed by third parties with or without user consent. This creates huge problems regarding privacy and security. The wireless communication poses huge risk for privacy and security as the data can be accessed by a third party or hacker without the user knowing it. The data is transferred to a third party using wireless communication which creates privacy risk. The person can be identifiable, health data and sensitive data may fall into the wrong hands. This data can be linked to an individual and it can be mined by third parties. The main issue is that an unauthorised third party accessing data without asking for permission from the user, creates privacy violations. An individual with health issues might use this wearable technology to monitor their health and there is a concern that data might be shared with a misappropriated third party which would be difficult to control. A user should be informed about the risk involving sharing their personal health data with an unauthorized third party while using wearable technology (Anaya, Alsadoon, Costadopoulos, & Prasad, 2018).

DISCUSSION

The first step of the data transition between the wearable devices should be security of data. The most important issue is to design key encryption methods while devices are communicating with each other (Zheng et al., 2014). The wearer should ensure that their private sensitive data should remain private, so the wearer will not introduce any vulnerability knowingly (W. Zhou & Piramuthu, 2014).

Health should be given the main importance by an individual, so the use of wearable devices to monitor our health would be easy to use and lead to a better quality of life (Darshan & Anandakumar, 2015). The wearable devices have good graphical user interface (Esteves, Ramalho, & De Haro) and good software to interact with devices. Data is stored on devices and then it is transferred to other devices like mobile, external USB or to the cloud (Bonfiglio & De Rossi, 2010). So the use of wearables has been adopted widely because of easy use and easy data storage.

Guidelines

The guideline for the wearable device users is listed below, and includes the factors identified in the research. The guideline shares some understanding about the importance of assuring the sensitive healthcare information security for consumers. Each element delivers some responsibility for consumers to assure information security. The details are derived based on present understanding of the field in general.

Health is most important to us. Now the medical data has become electronic so, therefore the health data security has become the most important type of data to protect. Nowadays hackers are targeting electronic health data. Personal health data is more important to protect than credit card numbers and bank account passwords. This is because electronic health data contains full name, date of birth, phone number, address, and place of work, insurance number information and financial data (Oliynyk, 2016).

The recommendations for protection is identified in Table 4 against the threats and vulnerabilities which is in Table 3.

Recommendations for protection	**Threats and vulnerabilities**
The Device should not be unattended for any reason. Keep the devices safe and lock the device when not in use (Das, Zeadally, et al., 2017).	5,6.11,14
Turn off the Bluetooth when not in use, the device can be easily hacked with Bluetooth (Bouhenguel, Mahgoub, & Ilyas, 2008b).	2,8,10,12
The sensitive health data and device information should not be sent or shared with anyone, it can be sent or shared with doctors and medical centres (Banerjee, Hemphill, & Longstreet, 2018).	5,6,8,13,15
It is easy to track the locations of the consumer, so turn off the GPS or location when not in use (Fowler, 2018).	1,5.6,14
Wearer should see the private policy made by the device's manufacturer (Ekelman, 1988).	8,9,11
Keep the devices fully charge to avoid unavailability of the device (Godfrey et al., 2018).	5,6,8,9
It is important to update software, operating system and application to avoid vulnerabilities and threats (J. A. Martin, 2017b).	4,7,8,9,10,12,13
The mobile is used to save data, so it should be protected well as it contains sensitive health data (Blumer & McGrath, 2018).	1,2,3,4,5,7,9,10,11,12,13,15
Before purchasing the consumer should know about the device and the privacy and security aspect like cryptograph, storage of data, usability and interface (Ekelman, 1988).	1,5,6,7,11,13,14,15
Consumer should be educated about the company policy and use of the data by the manufactures, about Bluetooth, GPRS and NFC (Pathirana, 2017).	1,2,3,11,12
Consumer should know how to use data and give access to people, they should know how to store data in a safe place. Many consumers are not too tech minded, so the manufacture should make it easy for them (Pathirana, 2017).	5,6,9,10,121,12,13,15
Protect the device from theft or losing, as it contains sensitive data and it should not fall into the wrong hands (Sun, Huai, Sun, Zhang, & Feng, 2008).	5,6,8,15

Use a password to protect the data, use strong password and authentication methods to secured data and devices (Diez et al., 2015).	2,3,4,5,6,8,9,14,15
Avoid downloading application forms unauthorised site and avoid using third-party application (Ching & Singh, 2016).	4,7,15
Avoid storing health data in many places, make minimal use of cloud and use external storage devices like pen drives and external hard drives (Tolson, 2018).	4,8,9

Table 4 - Recommendations for protection

Recommendations for manufacturers

The recommendation for manufacturers of wearable devices users is listed below. It was identified while doing research. The recommendation shares will help manufactures to protect sensitive health data. The details are derived and based on present understanding.

Recommendations for manufacturers
The manufacture should provide high power encrypted methods in the device.
The data collected in wearable devices should be encrypted so the attacker cannot regain the sensitive data.
If data is stored in peripheral devices like mobile, or on external drive or cloud, it should be encrypted.
When data is transferred from device to mobile via Bluetooth, GPS or NFC it should be encrypted while transferring.
The Manufacturer should provide the information about authentication and security measures and how and where the data is stored.
Manufactures should make their own application and avoid the use of third-party application.
There should be an authentication method when the data is being shared.
The device should have auto wipe feature
Manufacturers should try to make high power devices.

Table 5 - Recommendation for Manufactures

The main consideration for manufactures should be data protection from the wearable devices. Those who control this data in wearables device should know the data protection act and legislation, so they do not take any wrong steps. Data controllers must comply with the data protection legislation. The controller needs to inform the user if they are using their data to process. The user must be informed, what the data will be used for, unless processing is necessary for one of the limited reasons which is mentioned in the discussion of legislation. If the user does not allow the controller to process their data, then the controller should not process it. (Tozer, 2015).

In future there will be new vulnerability related to Bluetooth, WI-FI, data storage, data transmutation, collecting data, software and application.

CONCLUSION

This document explains different privacy and security problems in wearable devices which are used in healthcare. To understand regulation on wearable devices, a case study methodology was used. In this methodology the regulation and standards of USA, Australia and Europe were examined. HIPAA is an institute in USA, TGA is an institute in Australia and ISO is an institute in Europe which makes regulation and guidelines for those countries or continents. USA was selected because many technology companies are from USA. Australia was selected because we are living here. Europe was selected because of its recent interest shown towards privacy and security regulations. All these institutes have different regulations related to wearable devices.

The wearable devices have many privacy and security problems. The wearable devices are small in size so, an encryption method is not used, or a minimal level of encryption used, due to the small size of the device low memory and power. The wireless communication between devices or other smart devices is not secure. Sensors used in wearable devices can be targeted through different means. The data stored on wearables is not secure. It can be hacked easily and data which is stored in the cloud can be exposed to other people.

Wearables devices are growing fast these days, however, on the other hand privacy and security issues cannot be overlooked. The privacy and security issues might be a big obstacle for adopting wearable devices for the user. The awareness for privacy and security has been strengthened and the current situation of wearable devices epitomizes the threats to the user's privacy and security.

After studying and understanding this topic, it is clear that the current privacy and security issues associated with wearables devices have lack of security options and regulations. The new wearables devices have many benefits in our lives, but privacy and security should not be compromised. The user of the wearable device needs to protect their data and device from hacking and leaked information through any entity. Furthermore, the regulations for those devices need to catch up.

The future of wearable devices in healthcare looks promising. With this technology, the users can have their own health data at their fingertips, which gives them more empowerment, and they are equipped to track their own health. In some cases they can self-diagnosed their health problem. The user can share their health data with their doctor with better accuracy and in a structured way (medicaldirector, 2019). In future, this wearable technology will move one step forward compared to today, there will be embedded wearables in our cloths, skin patches and electronic skin. A small patch can measure the ECG and cardiac monitoring. Next generation smart watch can monitor real time diabetes with extracting blood out of the body. In future the patient does not need to carry hard copy files, all the important information would be stored in the wearable device (Crucius, 2018).

REFERENCES

Aira. (2018). Your Life, Your Schedule, Right Now. Retrieved from https://aira.io/

Al-Ameen Moshaddique, Liu Jingwei, & Kyungsup, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of medical systems, 36*(1), 93-101.

Al-Muhtadi, J., Mickunas, D., & Campbell, R. (2001). *Wearable security services.* Paper presented at the Proceedings 21st International Conference on Distributed Computing Systems Workshops.

Albert J. Mills, Durepos, G., & Wiebe, E. (2012). Encyclopedia of Case Study Research.

Anaya, L. S., Alsadoon, A., Costadopoulos, N., & Prasad, P. (2018). Ethical implications of user perceptions of wearable devices. *Science Engineering Ethics, 24*(1), 1-28.

Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015a). Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems, 1*(2), 99-109.

Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015b). Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems, 1*(2), 99-109.

Årsand, E., Muzny, M., Bradway, M., Muzik, J., & Hartvigsen, G. (2015). Performance of the first combined smartwatch and smartphone diabetes diary application study. *Journal of diabetes science, 9*(3), 556-563.

Ash, B. (2016). IoT and wearable devices: How standardisation is helping to drive market adoption. Retrieved from http://www.wearabletechnology-news.com/news/2016/apr/26/iot-and-wearable-devices-how-standardisation-helping-drive-market-adoption/

Atzori, L., Iera, A., & Morabito, G. J. C. n. (2010). The internet of things: A survey. *54*(15), 2787-2805.

Banerjee, S., Hemphill, T., & Longstreet, P. (2018). Wearable devices and healthcare: Data sharing and privacy. *The Information Society, 34*(1), 49-57.

Bansal, G., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision support systems, 49*(2), 138-150.

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *J The qualitative report, 13*(4), 544-559.

Biggs, J. (2017). New Bluetooth vulnerability can hack a phone in 10 seconds. Retrieved from https://techcrunch.com/2017/09/12/new-bluetooth-vulnerability-can-hack-a-phone-in-ten-seconds/

Billinghurst, M., & Starner. (1999). Wearable devices: new ways to manage information. *Computer, 32*(1), 57-64.

Blum, B. (2015a). Are Your Wearables Safe from Cyber-Security Threats? Retrieved from https://www.accenture.com/us-en/blogs/blogs-are-your-wearables-safe-from-cyber-security-threats

Blum, B. (2015b). How to Protect Your Wearables Implementation from Cyber-Security. Retrieved from https://www.accenture.com/us-en/blogs/blogs-how-to-protect-your-wearables-implementation-from-cyber-security-threats

Blumer, C., & McGrath, P. (2018). My Health Record agency adds 'reputation', 'public interest' cancellation options to app contracts. Retrieved from https://www.abc.net.au/news/2018-07-24/digital-health-agency-changes-my-health-record-app-contracts/10026644

Bonfiglio, A., & De Rossi, D. (2010). *Wearable monitoring systems*: Springer Science & Business Media.

Bouhenguel, R., Mahgoub, I., & Ilyas, M. (2008a). *Bluetooth security in wearable computing applications.* Paper presented at the 2008 international symposium on high capacity optical networks and enabling technologies.

Bouhenguel, R., Mahgoub, I., & Ilyas, M. (2008b). *Bluetooth security in wearable computing applications.* Paper presented at the High Capacity Optical Networks and Enabling Technologies, 2008. HONET 2008. International Symposium on.

Brandon, J. (2014). Wearable devices pose threats to privacy and security. Retrieved from https://www.foxnews.com/tech/wearable-devices-pose-threats-to-privacy-and-security

Cafazzo, J. A., Casselman, M., Hamming, N., Katzman, D. K., & Palmert, M. (2012). Design of an mHealth app for the self-management of adolescent type 1 diabetes: a pilot study. *Journal of medical Internet research, 14*(3).

Ching, K. W., & Singh, M. M. (2016). Wearable technology devices security and privacy vulnerability analysis. *International Journal of Network Security & Its Applications, 8*(3), 19-30.

Chuah, S. H.-W., Rauschnabel, P. A., Krey, N., Nguyen, B., Ramayah, T., & Lade, S. J. C. i. H. B. (2016). Wearable technologies: The role of usefulness and visibility in smartwatch adoption. *65*, 276-284.

Cooper, C. J. R. N. (2015). Latest security challenges: Wearables. *28*, 2015.

Crucius, S. (2018). Wearable Tech is Here to Stay with a Robust Presence in the Future Healthcare Industry. Retrieved from https://www.wearable-technologies.com/2018/06/wearable-tech-is-here-to-stay-with-a-robust-presence-in-the-future-healthcare-industry/

Darshan, K., & Anandakumar, K. (2015). *A comprehensive review on usage of Internet of Things (IoT) in healthcare system.* Paper presented at the 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT).

Das, A. K., Wazid, M., Kumar, N., Khan, M. K., Choo, K.-K. R., & Park, Y. (2017). Design of secure and lightweight authentication protocol for wearable devices environment. *IEEE journal of biomedical and health informatics, 22*(4), 1310-1322.

Das, A. K., Zeadally, S., Wazid, M., & Engineering, E. (2017). Lightweight authentication protocols for wearable devices. *J Computers, 63*, 196-208.

de Arriba-Pérez, F., Caeiro-Rodríguez, M., & Santos-Gago, J. (2016). Collection and processing of data from wrist wearable devices in heterogeneous and multiple-user scenarios. *Sensors, 16*(9), 1538.

Deborach Thoren-Peden, & Meyer, C. (2018). USA: Data Protection 2018. Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Diez, F. P., Touceda, D. S., Camara, J. M. S., & Zeadally, S. (2015). Toward self-authenticable wearable devices. *IEEE wireless Communications, 22*(1), 36-43.

Draper, S. (2018a). Hexoskin Smart Shirt Monitors and Records Heart Rate, Breathing and Movement. Retrieved from https://www.wearable-technologies.com/2018/06/hexoskin-smart-shirt-monitors-and-records-heart-rate-breathing-and-movement/

Draper, S. (2018b). How Data Breach is Inevitable in Wearable Devices. Retrieved from https://www.wearable-technologies.com/2018/10/how-data-breach-is-inevitable-in-wearable-devices/

Eadicicco, L. (2015). INTEL: Here's one of the biggest problems we need to solve with wearable tech. Retrieved from https://www.businessinsider.com.au/biggest-problems-with-wearable-tech-2015-2?r=US&IR=T

Ekelman, K. B. (1988). *New medical devices: Invention, development, and use*: National Academies.

Esteves, J., Ramalho, E., & De Haro, G. (2017). To improve cybersecurity, think like a hacker. *MIT Sloan Management Review, 58*(3), 71.

Fabietti, P., Benedetti, M. M., Bronzo, F., Reboldi, G., Sarti, E., & Brunetti, P. (1991). Wearable system for acquisition, processing and storage of the signal from amperometric glucose sensors. *The International Journal of Artificial Organs, 14*(3), 175-178.

FDA. (2015). Guidance for Industry and Food and Drug Administration Staff. *Mobile Medical Applications*.

FDA. (2018a). Classify Your Medical Device. Retrieved from https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/default.htm

FDA. (2018b). Guidances with Digital Health Content. Retrieved from https://www.fda.gov/MedicalDevices/DigitalHealth/ucm562577.htm

FDA. (2018c). Laws Enforced by FDA. Retrieved from https://www.fda.gov/regulatoryinformation/lawsenforcedbyfda/default.htm

Flynn, D. (2015). Challenges for power supplies in medical equipment: Ensuring patient and operator safety. *IEEE Power Electronics Magazine, 2*(2), 32-37.

Fowler, B. (2018). How to Turn Off Location Services on Your Smartphone. Retrieved from https://www.consumerreports.org/privacy/how-to-turn-off-location-services-on-your-smartphone/

Froggatt, T. J. (2011). An exploratory case study of a not for profit learning organisation.

Garcia-Mancilla, J., & Gonzalez, V. M. (2015). *Stress quantification using a wearable device for daily feedback to improve stress management.* Paper presented at the ICSH.

Gatzoulis, L., & Iakovidis, I. (2007). Wearable and portable eHealth systems. *IEEE Engineering in medicine and biology magazine, 26*(5), 51-56.

Godfrey, A., Hetherington, V., Shum, H., Bonato, P., Lovell, N., & Stuart, S. J. M. (2018). From A to Z: Wearable technology explained. *113*, 40-47.

Grandy, G. (2012). Encyclopedia of Case Study Research

Haghi, M., Thurow, K., & Stoll, R. (2017). Wearable devices in medical internet of things: scientific research and commercially available devices. *Healthcare informatics research, 23*(1), 4-15.

Harder, H. (2012). Explanatory Case Study

healthmanagement.org. (2017). Ransomware Seen as Medical Device Cybersecurity Threat. Retrieved from https://healthmanagement.org/c/it/news/ransomware-seen-as-medical-device-cybersecurity-threat

HHS. (2018). Security Rule Guidance Material.

Hiremath, S., Yang, G., & Mankodiya, K. (2014). *Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare.* Paper presented at the 2014 4th International Conference on Wireless Mobile Communication and Healthcare-Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH).

Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). *Towards an analysis of security issues, challenges, and open problems in the internet of things.* Paper presented at the 2015 IEEE World Congress on Services.

Hussain, M., Zaidan, A., Zidan, B., Iqbal, S., Ahmed, M., Albahri, O., & Albahri, A. (2018). Conceptual framework for the security of mobile health applications on android platform. *Telematics and Informatics, 35*(5), 1335-1354.

Jhajharia, S., Pal, S., & Verma, S. (2014). Wearable computing and its application. *International Journal of Computer Science Information Technologies, 5*(4), 5700-5704.

Jiang, H., Chen, X., Zhang, S., Zhang, X., Kong, W., & Zhang, T. (2015). *Software for wearable devices: Challenges and opportunities.* Paper presented at the 2015 IEEE 39th Annual Computer Software and Applications Conference.

Jovanov, E., Milenkovic, A., Otto, C., & De Groen, P. C. (2005). A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. *Journal of NeuroEngineering rehabilitation, 2*(1), 6.

Kargl, F., Lawrence, E., Fischer, M., & Lim, Y. Y. (2008). *Security, privacy and legal issues in pervasive ehealth monitoring systems.* Paper presented at the 2008 7th International Conference on Mobile Business.

Karimi, K., Atkinson, G., & ARM. (2013). What the Internet of Things (IoT) needs to become a reality. *White Paper, FreeScale*, 1-16.

Khan, I. M., Jabeur, N., Khan, M. Z., & Mokhtar, H. (2012). *An overview of the impact of wireless sensor networks in medical health care.* Paper presented at the The 1st International Conference on Computing and Information Technology (ICCT).

Kim, S.-C., & Lim, S.-C. (2015). Transferring data from smartwatch to smartphone through mechanical wave propagation. *Sensors, 15*(9), 21394-21406.

Korhonen, I., Parkka, J., & Van Gils, M. (2003). Health monitoring in the home of the future. *IEEE Engineering in medicine and biology magazine, 22*(3), 66-73.

Kraft, J. C. (2018). What My Smart Shoes Taught Me. Retrieved from https://medium.com/neodotlife/under-armour-hovr-sonic-connected-978b2a0f7ad

Lee, K. (2009). Wearable health technology and HIPAA: What is and isn't covered. Retrieved from https://searchhealthit.techtarget.com/feature/Wearable-health-technology-and-HIPAA-What-is-and-isnt-covered

Lee Linda, Egelman Serge, Lee Joong Hwa, & David, W. (2015). Risk perceptions for wearable devices. *J arXiv preprint arXiv:.05694*.

Lemos, R. (2016). Watch out: 5 reasons smartwatches need smarter security. Retrieved from https://techbeacon.com/app-dev-testing/watch-out-5-reasons-smartwatches-need-smarter-security

Li Han, Gupta Ashish, Zhang Jie, & Rathindra, S. (2014). Examining the decision to use standalone personal health record systems as a trust-enabled fair social contract. *Decision support systems, 57*, 376-386.

Li, I., Dey, A., & Forlizzi, J. (2010). *A stage-based model of personal informatics systems.* Paper presented at the Proceedings of the SIGCHI conference on human factors in computing systems.

Liu, J., & Sun, W. (2016). Smart attacks against intelligent wearables in people-centric internet of things. *IEEE Communications Magazine, 54*(12), 44-49.

Lloyd, A. (2014). Wearable Tech and Personal Security Breaches: 6 Things to Know. Retrieved from https://blog.hotspotshield.com/2014/12/16/wearable-tech-and-personal-security-breaches/

Lmberis, A., & Dittmar, A. (2007). Advanced wearable health systems and applications-research and development efforts in the European Union. *IEEE Engineering in medicine and biology magazine, 26*(3), 29-33.

Locke, C. (2014). Top 3 security tips for wearable devices. Retrieved from https://thedigitalbankingclub.com/blogs/4767-top-3-security-tips-for-wearable-devices

Locke, C. (2014). Top 3 security tips for wearable devices. *Retrieved November, 28*, 2015.

Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity authentication and capability based access control (iacac) for the internet of things. *Journal of Cyber Security and Mobility, 1*(4), 309-348.

Martin, J. A. (2017a). 10 things you need to know about the security risks of wearables. Retrieved from https://www.cio.com/article/3185946/10-things-you-need-to-know-about-the-security-risks-of-wearables.html

Martin, J. A. (2017b). 10 things you need to know about the security risks of wearables. Retrieved from https://www.cio.com/article/3185946/10-things-you-need-to-know-about-the-security-risks-of-wearables.html

Martin, T., Jovanov, E., & Raskovic, D. (2000). *Issues in wearable computing for medical monitoring applications: a case study of a wearable ECG monitoring device.* Paper presented at the Digest of Papers. Fourth International Symposium on Wearable Computers.

medicaldirector. (2019). The future of wearable devices in healthcare. Retrieved from https://www.medicaldirector.com/news/future-of-health/2019/02/new-report-reveals-the-future-of-wearable-devices-in-healthcare

Molisch, A. F., Balakrishnan, K., Chong, C.-C., Emami, S., Fort, A., Karedal, J., . . . Siwiak, K. (2004). IEEE 802.15. 4a channel model-final report. *IEEE P802, 15*(04), 0662.

Nina Kostyukovsky, D. P. (2018). Regulating Wearable Devices in the Healthcare Sector. Retrieved from https://www.americanbar.org/groups/health_law/publications/aba_health_esource/2014-2015/may/devices/

Oliynyk, M. (2016). Why is healthcare data security so important? Retrieved from https://www.protectimus.com/blog/why-is-healthcare-data-security-so-important/

Pantelopoulos, A., & Bourbakis, N. G. (2010). A survey on wearable sensor-based systems for health monitoring and prognosis. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 40*(1), 1-12.

Patel, M. S., Asch, D. A., & Volpp, K. G. (2015). Wearable devices as facilitators, not drivers, of health behavior change. *Jama, 313*(5), 459-460.

Pathirana, H. P. A. (2017). *Creation of a Socio-Technical Framework for Securing Personal Monitoring Devices (PMD).* Masters by Coursework, Thesis (Masters),

Perera, C., Liu, C. H., & Jayawardena, S. (2015). The emerging internet of things marketplace from an industrial perspective: A survey. *IEEE Transactions on Emerging Topics in Computing, 3*(4), 585-598.

Reis, R. (2009). Strengths and limitations of case studies. *on http://cgi. stanford. edu/~ dept.*

Roos, A. (2009). *The law of data (privacy) protection: a comparative and theoretical study.*

Ross, D. A. (2001). Implementing assistive technology on wearable computers. *J IEEE Intelligent systems, 16*(3), 47-53.

Ruck, A. (2015). Information and Stakeholders' Day on Smart Wearables.

Ruck, A., & Limited, C. (2015). Information and Stakeholders' Day on Smart Wearables. *Organised by the European Commission, Directorate General for Communications Networks, Content and Technology, DG CONNECT*(11-12-2015), 15-17.

Saa, P., Moscoso-Zea, O., & Lujan-Mora, S. (2018). *Wearable Technology, Privacy Issues.* Paper presented at the International Conference on Information Theoretic Security.

Sano, A., & Picard, R. W. (2013). *Stress recognition using wearable sensors and mobile phones.* Paper presented at the 2013 Humaine Association Conference on Affective Computing and Intelligent Interaction.

Sawh, M. (2017). Myontec shifts its smart clothing focus to elite athletes. Retrieved from https://www.wareable.com/sport/myontec-mbody-janne-pylvas-interview-8668

Shah, S. (2018). How to Check Your Health With a Smartwatch. Retrieved from https://www.healthcareguys.com/2018/10/23/how-to-check-your-health-with-a-smartwatch/

Shrestha, P., & Saxena, N. J. A. C. S. (2018). An offensive and defensive exposition of wearable computing. *50*(6), 92.

Shreyas. (2019). Connected Wearable Patches Market to Witness Growth Acceleration During 2019-2025| G-Tech Inc., Proteus Digital Health, Chrono Therapeutics, Blue Spark Technologies, KENZEN, Gentag Inc., Preventice Solutions. Retrieved from https://themarketresearchnews.com/2019/05/23/connected-wearable-patches-market-to-witness-growth-acceleration-during-2019-2025-g-tech-inc-proteus-digital-health-chrono-therapeutics-blue-spark-technologies-kenzen-gentag-inc-preventice-so/

Siboni, S., Shabtai, A., Tippenhauer, N. O., Lee, J., & Elovici, Y. (2016). Advanced security testbed framework for wearable IoT devices. *ACM Transactions on Internet Technology, 16*(4), 26.

Singh, S., Rai, R. & Technologies, I. (2014). A Review Report on Security Threats on Database. *5*(3), 3215-3219.

Snell, E. (2017). How Do HIPAA Regulations Apply to Wearable Devices? Retrieved from https://healthitsecurity.com/news/how-do-hipaa-regulations-apply-to-wearable-devices

Sorber, J., Shin, M., Peterson, R., Cornelius, C., Mare, S., Prasad, A., . . . Kotz, D. (2012). *An amulet for trustworthy wearable mHealth.* Paper presented at the Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications.

Standards. (2016). Internatnal Updates Retrieved from https://www.standards.org.au/getmedia/b879824d-df0d-4177-858b-1b221e4a51f7/International-update-February-2016.aspx

Sultan, N. (2015). Reflective thoughts on the potential and challenges of wearable technology for healthcare provision and medical education. *International Journal of Information Management, 35*(5), 521-526.

Sumra, H. (2018). How FDA approval affects your wearables, and how it's going to change. Retrieved from https://www.wareable.com/wearable-tech/fda-wearables-state-of-play-239

Sun, D.-Z., Huai, J.-P., Sun, J.-Z., Zhang, J.-W., & Feng, Z.-Y. (2008). A new design of wearable token system for mobile device security. *IEEE Transactions on Consumer Electronics, 54*(4), 1784-1789.

Swan, M. (2012). Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. *Journal of Sensor Actuator networks, 1*(3), 217-253.

Taylor, N. P. (2019). Current Health's wearable vital sign monitor gets FDA nod. Retrieved from https://www.medtechdive.com/news/current-healths-wearable-vital-sign-monitor-gets-fda-nod/547779/

Techopedia.com. (2018). What is a Wearable Device? Retrieved from https://www.techopedia.com/definition/31206/wearable-device

TGA. (2017a). Complying with Wearable Health Device Regulation. Retrieved from https://www.tga.gov.au/sites/default/files/complying-with-wearable-health-device-regulation.pdf

TGA. (2017b). Medical devices regulation: an introduction. Retrieved from https://www.tga.gov.au/sme-assist/medical-devices-regulation-introduction

Tolentino, M. (2013). 4 Security Challenges for Fitbit, Google Glass + Other Wearable Devices. Retrieved from https://siliconangle.com/2013/05/30/4-security-challenges-for-fitbit-google-glass-other-wearable-devices/

Tolson, B. (2018). Where Should Healthcare Data Be Stored In 2018 — And Beyond? Retrieved from https://www.healthitoutcomes.com/doc/where-should-healthcare-data-be-stored-in-and-beyond-0001

Tozer, D. (2015). Legal: The laws and regulations of wearable devices. Retrieved from http://www.wearabletechnology-news.com/news/2015/sep/10/where-law-stands-wearable-devices/

Tröster, G. (2005). The agenda of wearable healthcare. *Yearbook of medical informatics, 14*(01), 125-138.

Turner, R. (2017). Owlet Smart Sock prompts warning for parents, fears over babies' sensitive health data. Retrieved from https://www.abc.net.au/news/2017-09-12/owlet-smart-sock-prompts-warning-for-parents-privacy-concerns/8893104

Upton, D. (2015). 5 essential wearable tech security tips. Retrieved from https://betanews.com/2014/12/09/5-essential-wearable-tech-security-tips/

Urias, V. E., Van Leeuwen, B., Stout, W. M., & Lin, H. (2018). *Applying a Threat Model to Cloud Computing.* Paper presented at the 2018 International Carnahan Conference on Security Technology (ICCST).

Wellocracy. (n.d.). Wearable Activity Devices Comparison Chart. Retrieved from http://www.wellocracy.com/wearable-activity-trackers/wearable-activity-tracker-chart/

Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers, 17*(2), 261-274.

Wright, R., & Keith, L. (2014). Wearable technology: If the tech fits, wear it. *Journal of Electronic Resources in Medical Libraries, 11*(4), 204-216.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 798.

Yan, V. (2019). Hi-tech iTBra a breakthrough for Asian women at high risk of breast cancer. Retrieved from https://www.scmp.com/lifestyle/health-wellness/article/2180728/hi-tech-itbra-breakthrough-asian-women-high-risk-breast

Yao, J., Warren, S. J. J. o. c. m., & computing. (2005). Applying the ISO/IEEE 11073 standards to wearable home health monitoring systems. *19*(6), 427-436.

Zainal, Z. (2007). Case study as a research method. *Jurnal Kemanusiaan, 5*(1).

Zheng, Y.-L., Ding, X.-R., Poon, C. C. Y., Lo, B. P. L., Zhang, H., Zhou, X.-L., . . . Zhang, Y.-T. (2014). Unobtrusive sensing and wearable devices for health informatics. *IEEE Transactions on Biomedical Engineering, 61*(5), 1538-1554.

Zhou, J., Cao, Z., Dong, X., & Lin, X. (2015). Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions, and future directions. *IEEE wireless Communications, 22*(2), 136-144.

Zhou, W., & Piramuthu, S. (2014). *Security/privacy of wearable fitness tracking IoT devices.* Paper presented at the 2014 9th Iberian Conference on Information Systems and Technologies (CISTI).