EAI Endorsed Transactions
on Pervasive Health and Technology
Research Article EAI.EU

Security and Privacy Issues with IoT in Healthcare

Anil Chacko[1], Thaier Hayajneh[1,*]

[1]Fordham Center for Cybersecurity, Fordham University, New York, NY, USA

Abstract

In healthcare, the Internet of Things (IoT) offers many benefits, including being able to monitor patients more closely and using data for analytics. When it comes to IoT for medical device integration, the focus is shifted towards the consumer end, such as glucose meters, blood pressure cuffs, and other devices designed to record data on patient vital signs. This enables healthcare providers to automatically collect information and apply decision support rules to allow for earlier intervention in the treatment process. Unfortunately, medical companies often do not consider the security risks of connecting these devices to the internet. There is a possibility that a zero-day exploit in a medical device can be used to injure or even kill someone without being detected. The rise in hackable medical devices has forced the FDA to issue formal guidance on how medical device makers should handle reports about cyber vulnerabilities. This paper aims to explore the role of IoT in healthcare, vulnerabilities, attacks, and security issues and solutions.

Received on 29 April 2018; accepted on 08 June 2018; published on 23 July 2018

Keywords:

doi:10.4108/eai.13-7-2018.155079

1. Introduction

The internet of things (IoT) is the networking of physical devices that are both connected and smart. These devices are embedded with software, sensors, and network connectivity that enables them to collect and exchange data. An IoT can be controlled remotely across existing network infrastructure, this creates an opportunity for more direct integration of devices into computer-based systems which results in improved efficiency, and accuracy. This in turn provides an economic benefit to those who use it.

An IoT device that use sensors and actuators, the technology becomes a part of cyber-physical systems. These types of technologies include smart grids, smart homes where it is used to control and automate lighting, heating and cooling with a smart thermostat like the Nest Thermostat. Appliances such as washers, dryers, ovens or refrigerators can use Wi-Fi for remote monitoring. There are automobiles with built-in sensors, field operation devices that can assist firefighters in search and rescue operations. Each of these things are uniquely identifiable via the embedded computing system, but they can also easily interoperate within the existing Internet infrastructure. These devices collect useful data with the help of various existing technologies and then autonomously move the data between other devices. Experts are estimating that by the year 2020 the IoT will consist of almost 50 billion objects. A significant portion of these will be medical devices, from pacemakers to infusion pumps, mobile medical workstations, in-home monitors, and personal fitness devices.

When it comes to healthcare the "Things," in the Internet of Things, can refer to a wide variety of devices such as heart monitoring implants, infusion pumps that are used in hospitals to deliver a pre-programmed level of fluids into a patient. There are also millions of other devices like pacemakers, insulin pumps, and cochlear implants. Some of these devices only send information via a wireless connection like a pace maker, while others can send and receive information. There are also devices know as wearables, like the Apple watch or the Fitbit, that can track vital information including your daily activity information, including the number of steps taken or calories burned. At some point this data is synced with the watch or another device for data analysis and to keep a history.

The increase of IP-connected sensors in hospital equipment and in patients gives us the opportunity

*Corresponding author. Email: thayajneh@fordham.edu

to eliminate unnecessary waste and save lives. IoT gives the healthcare sector the opportunity to redefine the way things are done, but making this happen will involve enormous difficulty. Tying together all the disparate systems in the healthcare environment will be a challenge. In addition, there will always be the security concerns as to how these devices are secured. How easy is it for an attacker to take control of these devices?

2. The Role of IoT in Healthcare

Healthcare is defined as the act of taking preventative or necessary procedures to improve a person's well-being. This may be done with surgery, the administering of medicine, or other alterations in a person's lifestyle. These services are typically offered through a health care system made up of hospitals and physicians.

There are several areas in healthcare that IoT is playing an important role.

- Elder care, which involves tracking elderly residence/patients at nursing home and hospital
- Data gathering, which is the most mature area in healthcare, it involves many equipment that we see at bedside in hospitals like the EKG monitor, this is an area that continues to expand with new innovations happening in the world of IoT
- Real-time location is used to track people and assets at a lower cost

As the presence of IoT in the healthcare sector increases, it is going to benefit both patients and health-care providers. Treatments that patients receive can be enhanced by remote monitoring and communication, areas where IoT can play a big role.

Another use of healthcare IoT is mobile medical applications or wearable devices that allow patients to capture their health data. Much of this can be attributed to the data revolution which is empowering us to live healthier lives by using connected devices such as tablets, wearables and hand-held devices. The analysis of the data collected through electronic medical records, diagnostic information gathered through imaging equipment and hand-held personal devices will enhance the decision-making powers. This will allow patients to take a more active role in managing their personal health.

In the future, this data-rich personalized analysis of our health will become the standard. Patients will be provided with tailor-made strategies to fight illness. From the data generated, we will learn how to improve our wellbeing and we will be motivated to take control of our life. There is a whole new industry around clinical decision support software, a growing sector related to IoT that boosts the role of connected devices by tying their use more directly to clinical decisions.

The Food and Drug Administration (FDA) has already done quite a bit of work in establishing universal device identifiers for medical devices in IoT applications. There should be tagging of the metadata generated by connected devices that would allow data to be closely tracked as it travels between devices or between devices and networks. Doctors do not have to wonder about the data. They will be able to trust this data and will know that it is really from their patient.

The Healthcare sector remains one of the fastest to adopt the Internet of Things. Integrating IoT features into medical devices improves the quality and effectiveness of service rendered, this is very valuable for patients who have chronic conditions, the elderly, and those requiring constant care. According to a study conducted by McKinsey Global Institute, spending on the Healthcare IoT solutions will reach $1 trillion by 2025 (see Fig.1). It is possible that this could set the stage for highly personalized, accessible, and on-time healthcare services for everyone.

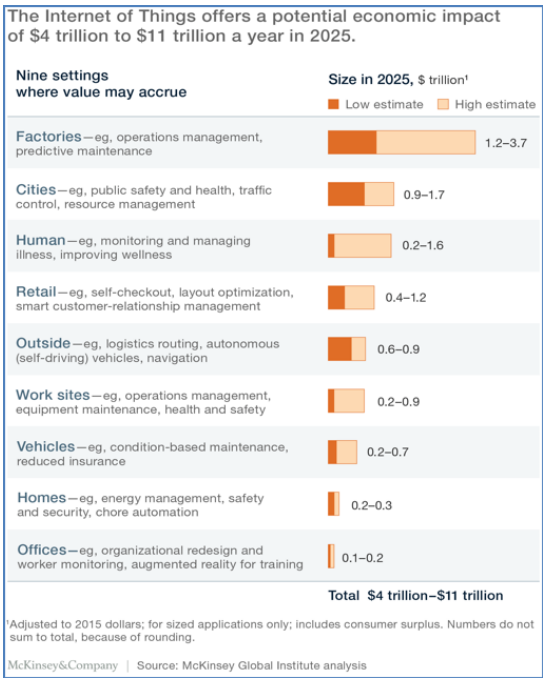

Figure 1. Economic impact of IoT Devices by 2025.

Hospitals have been adopting the Internet of Things for many years. It is very common to see IoT devices in patient rooms, electronic medical records and other cloud-based resources. At most healthcare organizations networking new devices is an ongoing initiative. However, the biggest challenge is the interoperability of devices which can lead to a network being exposed to new security vulnerabilities and additional risk.

The BYOD devices are a potential issue, without proper monitoring they can very easily become part of a network and represent an immense target for attack. Since it is difficult to control the quality of the operating systems or the code that runs on these devices, organizations must monitor the use of these devices, log when they access or extract data.

As healthcare systems become interconnected, especially as numerous wireless medical devices start connecting to web-enabled IT systems they become increasingly vulnerable. This vulnerability is not just from malicious hackers, but from other threats such as malware and the computer virus.

3. DDoS with IoT Devices

Distributed denial of service (DDoS), is an attack where multiple compromised systems are used to target a single system causing a denial of service and causing that system to crash. There are many different methods used to launch these attacks, one way is to use malicious botnets. Recently the source code for a malware that can build botnets out of IoT products was publicly released. Since then, the total number of IoT device infected by the Mirai malware has jumped to 493,000 from 213,000, according to internet provider Level 3 communications (6). Now imagine a scenario with a million compromised IoT devices and the collateral damage that can cause, especially if some of these IoTs are medical devices.

While some connected medical devices, like pacemakers, can only send information, others, can send and receive data. This leaves some patients vulnerable to a hacker trying to harm them or use their device as a portal to access medical data.

In June 2015, Billy Rios, a security researcher who helps the Department of Homeland Security proved he could remotely administer a lethal dose of drugs through a patient's insulin pump. He and his colleague were able to figure out the passwords after acquiring embedded software and technical manuals from several vendors. He was also able to hack pre-programmed passwords from hundreds of devices.

The Food and Drug Administration, which regulates the sale of medical devices, has been issuing formal guidelines on the issue. They have published new recommendations on how medical device makers should take cyber-security attacks into account.

4. Providing Improved Patient Care

Compared to other developed economies the United States spends far more on healthcare each year. Government projections predict that the current spend of 18% of total GDP will only continue to rise in the coming years. US is desperately in need to reduce healthcare costs, and analysts think the Internet of Things (IoT) is something that will help in a major spending reduction in the future. Analysts at Goldman Sachs are predicting that digital healthcare will revolutionize the industry, both by increasing access to diagnostic, treatment, and preventative care, and by dramatically reducing costs.

Keeping track of high risk patients is a major challenge in keeping health care cost down. Chronic disease management accounts for about 1/3 of all US healthcare spending, and most of that spending is related to heart disease, asthma and diabetes. Remote monitoring will enable healthcare providers to frequently keep track of high risk patients. Analysts see the opportunity for $305 billion in savings from digital healthcare, as much as $200 billion of that could come from chronic disease management, largely by eliminating redundant and wasteful expenses.

IoT in healthcare can also be known as IoMT (internet of Medical Things), In this case IoMT is a collection of medical devices and corresponding applications that connect to the healthcare IT systems through a computer network (Fig. 2). IoMT is basically medical equipment with Wi-Fi connectivity that communicate with one another. These devices can link with cloud storage provided by Amazon AWS to store captured data that can be analyzed later.

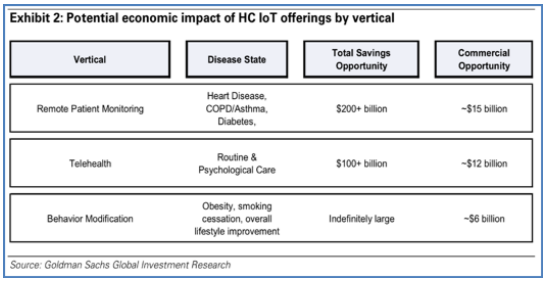
Exhibit 2: Potential economic impact of HC IoT offerings by vertical

Vertical	Disease State	Total Savings Opportunity	Commercial Opportunity
Remote Patient Monitoring	Heart Disease, COPD/Asthma, Diabetes,	$200+ billion	~$15 billion
Telehealth	Routine & Psychological Care	$100+ billion	~$12 billion
Behavior Modification	Obesity, smoking cessation, overall lifestyle improvement	Indefinitely large	~$6 billion

Source: Goldman Sachs Global Investment Research

Figure 2. The potential impact of IoT in Healthcare

Remote patient monitoring (RPM) is one area where IoT is being used in healthcare. RPM which is sometimes referred to as telehealth is a type of healthcare that allows patients to use a mobile device to perform a routine test and then send the data back to their healthcare provider in real-time. This technology includes monitoring devices like a glucose meter used by a patient who is diabetic or blood pressure and heart monitor for cardiac care patients. This information can be delivered to a physician's office by a software applications that can be installed on smartphone or a tablet. This technology will reduce hospital readmissions or physician visits. This kind of treatment spares patients from traveling to a hospital or physician's office whenever they have a medical question or change in their condition. It also cuts down the cost of keeping a patient in hospital setting which can be very expensive. The Kaiser Family Foundation

study found that the average daily cost for a single patient was over $1,700 in 2013.

The BodyGuardian Remote Monitoring System is a system that provides this functionality, it helps the physicians refine the care given while allowing the patients to live their life without restrictions. The system addresses security requirements in several ways, first it separates patient identification information and observation data. Then the system encrypts data on the device, during transmission and in storage. This technology is used quite often with the two groups that requires high level of medical need, those that are chronically ill or the elderly. The medical providers can keep a close watch on their patient's conditions and intervene if needed. FCC's National Broadband Plan mentions that the remote patient monitoring technology along with electronic health record can save the healthcare industry $700 billion over 15 to 20 years.

Mobile Health (mHealth) Device that can be worn by patients also known as mHealth devices can send information to their caregivers. Infusion pumps that connect to analytics dashboard and patient beds in the hospital have numerous sensors that measures the vital signs of the patient. With connectivity, care can be delivered anywhere, including at home, thereby lowering costs while improving the patient experience. Analysts believe that the mHealth technology market will grow at an annual rate of nearly 55% to reach $21.5 billion by the year 2018 (4).

5. Medical Device Integration

A *pacemaker* is a medical device invented in the 1920s, which is implanted under a person's skin, with wiring going down to their heart, it helps regulate abnormal heart rhythms. They have evolved over time, shrinking in size, and advancements in recent years has allowed more digital capabilities, especially when it comes to transmitting data from the patient's body to nearby access points, or remote servers. In today's world of IoT hacking, this can raise serious concerns if the pacemakers are not using proper security.

A modern pacemaker has the capability to collect information about patients, and transmit it via Wi-Fi to an access point or medical devices used during hospital checkups. The access point devices, which collect information about the patient's health while at home, sends the data to remote servers. Pacemakers that can send data via the Internet can help patients with mobility issues. However, the communications protocols used when sending the data to remote servers is very trivial and is susceptible of being hacked.

Implantable cardioverter defibrillator (ICD) - An ICD is a battery-powered device placed under the skin that keeps track of your heart rate. More than 135,000 patients receive these defibrillators each year to prevent sudden heart attacks.

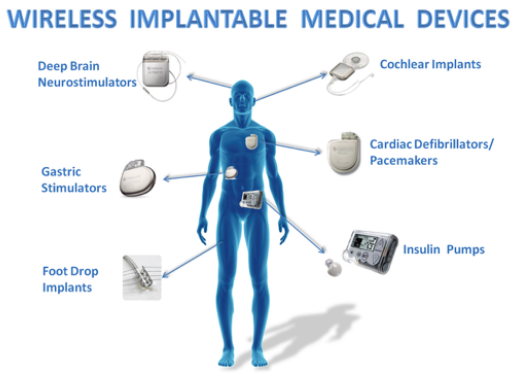

Figure 3. Example IoT medical devices on a patient's body.

An *insulin pump* can be programmed to releases small doses of insulin continuously, or a single dose close to mealtime to control the rise in blood glucose the main sugar found in the blood and the body's main source of energy. This delivery system most closely mimics the body's normal release of insulin.

Concern about the vulnerability of medical devices like a pacemaker, ICDs, insulin pumps, defibrillators, fetal monitors and scanners is growing as healthcare facilities increasingly rely on devices that connect with each other (See Fig. 3), with hospital medical record systems and with the Internet. So far there have been no confirmed reports of cyber criminals gaining access to a medical device and harming patients, the Department of Homeland Security is investigating potential vulnerabilities in about two dozen devices. Hospital medical devices may be vulnerable to hackers simply because they can be the weak link that gives a criminal access to a hospital's data system - especially if the devices haven't been updated with the latest security patches.

6. Security and Privacy Concerns

In late 2015, two security researchers discovered over 68,000 medical systems that were exposed online, and 12,000 of them belonged to one healthcare organization (8). The major concern with this discovery was that these devices were connected to the Internet through computers running very old versions of Windows XP, a version of the OS which is known to have lots of exploitable vulnerabilities. These devices were discovered by using Shodan, a search engine that can find IoT devices online that are connected to the internet. These are easy to hack via brute-force attacks and using hard-coded logins. During their research, the two experts found anesthesia equipment, cardiology devices, nuclear medical systems, infusion systems,

pacemakers, MRI scanners, and other devices all via simple Shodan queries.

The two security experts created honeypots, which are special servers that appears as medical devices. These devices had fake medical data and real vulnerabilities, but they also had a logging component. When the researchers reviewed, the logs gathered by these honeypots, they found that attackers managed to authenticate via SSH on these fake medical devices over 55,000 times, they even left 299 malware payloads. There were also 24 cases when the attackers successfully exploited the same vulnerability that was previously exploited by the Conficker infections. The researchers also found out that in most cases the attackers did not realize what they had hacked and left an infected machine behind as a part of their botnets. If the hackers figure out that the devices could lead them to other servers with more sensitive information, they wouldn't hesitate to conduct a more sophisticated attack to get this valuable information. They could also use the devices to spread dangerous malware inside a hospital's IT infrastructure (8).

There has been a rise in data security and liability risks in the healthcare sector because of IoT. The Internet of Things brings many of the same security and privacy issues, but it is a much greater risk because these devices act automatically. Doctors are now able to program ICDs to monitor a patient's heart condition. These devices can deliver data about that person's heart rhythms to a doctor. It can also send the right level of electrical shock to get the heart beating properly. Researchers have been able to demonstrate how a malicious hacker can trigger the device to malfunction, delivering a dangerous shock.

The Showtime television series Homeland had an episode where hackers disabled the pacemaker of the vice president to assassinate him. Former Vice President Dick Cheney in an interview with "60 Minutes," revealed that when he had a device implanted to regulate his heartbeat, he had his doctors disable its wireless capabilities to prevent against a possible assassination attempt.

7. Medjacking

It is possible that hackers could tamper with medical devices to harm individuals, but we haven't seen anything like that yet. Devices are usually hacked so attackers can get into larger medical systems and steal protected health information. In June 2015, a report was released by TrapX, a security company which revealed that most healthcare organizations are vulnerable to medical device hijacking also called "medjacking". The report provided details about incidents of medjacking in three hospitals. In the first case, a blood gas analyzer infected with two different types of malware was used to steal passwords for other hospital systems, and confidential data was being sent to computers in Eastern Europe. At another hospital, the radiology department's image storage system was used to gain access to the main network, sensitive data was retrieved and sent to a location in China. In the third case, hackers used the vulnerability in a drug pump to gain access to the hospital network. Stolen medical identities are much more valuable than the price of a stolen credit card number. The current state of security in many medical devices allow hackers easy access to steal massive numbers of sensitive data from healthcare provider's systems (10).

Insulin pumps (Fig. 4) are medical devices that patients attach to their bodies that injects insulin through catheters. The Animas OneTouch Ping, was launched in 2008, is sold with a wireless remote control that patients can use to order the pump to deliver a dose of insulin, which is typically worn under clothing and can be awkward to reach. Johnson & Johnson recently informed patients that it has learned of a security vulnerability in one of its insulin pumps that a hacker could exploit to overdose diabetic patients with insulin. This system is vulnerable because communications are not encrypted, to prevent hackers from accessing the device. Hackers can force the device to deliver unauthorized insulin injections. The chances of such a hack happening is very low. However, this is the first time a manufacturer of medical devices had issued such a warning to patients about a cyber vulnerability. This revelation has increased concerns about possible bugs in pacemakers and ICDs. J&J is warning customers and providing advice to fix the issue.

Figure 4. Example vulnerable drug pump.

In another case, the FDA last year issued multiple warnings about cyber bugs in infusion pumps from Hospira, which was acquired by Pfizer Inc. They have

been aware of the security issue for a while, and have issued guidelines for manufacturers to make their device more secure. However, this is the first-time FDA has issued a warning for a medical device based on cyber security risk. In Aug 2015, the FDA recommended that all hospitals in California and across the country should stop using a medical device that is vulnerable to cyber-attacks. This device is an infusion pump that delivers medications or nutrients to patients. A hacker can access and change the drug dosage to give a patient too little or a lethal amount.

8. Data Covered Under HIPAA

Connected devices offer many advantages, however, these devices also pose increased risks to privacy and security. Some possible risks include:

- Enabling unauthorized access that can lead to misuse of personal information
- Facilitating attacks on other systems
- Creating risks to personal safety
- Privacy risks that arise from the collection of personal information, locations and physical conditions.

There is also concern among users of the mHealth and wearable technology about privacy and ownership of the data. Countries have laws in place to protect patient data but it is not consistent, and there is a great deal of variability. In the United States HIPAA governs the security and privacy of health information, but it only applies to health care. This allows the makers of mobile health (mHealth) devices to share the user-generated data without the knowledge of the user.

A recent study by U.S. Federal Trade Commission tested 12 health and fitness applications and discovered these applications were sending consumer data to 76 third-party companies (3). Some of the data shared included the phone's unique device identifier (UDID) and its media access control address or the MAC address. They also shared other consumer information like the user's running route, dietary habits, sleep patterns, exercise information, gender, zip codes. A separate report by Privacy Rights Clearinghouse also indicated that 40% of 43 fitness applications collected high-risk data, including addresses, financial information, full name, health information, location and date of birth. The report also found 55% of those 43 applications shared data with third-party analytical services that could potentially link data from the fitness and health applications to other applications that contain identifying information about the user (5).

Organizations that are covered by HIPAA are called covered entities, which means malicious entities can often do whatever they want with someone's data, if those potential actions are included in the terms and conditions-which are rarely read by users.

The data tracked and collected by wearable health technology that many people think should be covered by HIPAA, in many cases are not. If someone simply goes to the store and buys a Fitbit, for example, it isn't covered by HIPAA. Therefore, the data collected is not bound by or protected by the regulation. However, if a person receives a wearable device through their hospital or doctor, the healthcare data that device collects is covered by HIPAA. At least the data that HIPAA defines as protected healthcare information (PHI) is safeguarded.

9. How to Secure IoT in Healthcare

Healthcare communities have accepted the fact that IoT will be a part of their future. They understand that digitizing and streamlining the sharing of health data will allow them to gain efficiency and will result in significant cost savings.

There are several basic security actions that providers and manufacturers of IoT devices can take including *encryption* and conducting a *secure boot*. A secure boot is making sure that when a device is turned on, none of its configurations have been modified (7).

It is a challenge for CIOs and CISOs as they continue to figure out ways to manage the risks of IoT and capture the benefits. To prepare and remain as secure as possible, there are steps that they should take.

- Security measures should be incorporated into the design of the IoT device, this includes conducting a risk assessment before the device is released for use in the market, authentication measures should be built into the device
- Make sure that authentication is properly followed, device access is limited, firmware being sent to the device is verified, and device-to-device communication is monitored
- A defense in depth strategy should be implemented, where several layers of security is in place to protect against specific risks
- Ensure there are proper access control in place that limit unauthorized access to data, the IoT devices and the networks
- Test the security of the IoT device before it is put into production and monitor the security of the device throughout its life cycle
- Establish culture of security, where the employees are trained to recognize vulnerabilities

10. Conclusion

So far, there are no known cases in which malicious hackers have attacked a pacemaker, but researchers have proved it's possible. In addition, research firm Forrester has predicted that in the near future we will see ransomware for a medical device or wearable. The systems those devices connect to in hospitals often have a lot of legacy equipment that are running outdated operating systems and software that cannot be updated.

In the transient environment of a healthcare provider devices can enter in many ways, many times how they enter are unknown, BYOD is a good example. When this happens, it becomes difficult to figure out the life cycle management of that device and identify the operating system. Standalone devices that attach to the network may have developed networks and connectivity glitches. Since these devices do not come through normal channels there is a lack of awareness of these vulnerabilities that attackers could take advantage.

When a vendor, rogue IT staff member or even a hacker can put standalone devices on an isolated network. Many of these devices in healthcare lack evidence capture and forensic logging capabilities, therefore there is no way to track what is happening.

It is understood that IoT devices are her to stay because they help cut cost and make it easier to perform important functions. It is important to make sure that the networks run automated work flows, give quick access to critical information while keep everything secure. This can be accomplished with enforceable security policies and implementing solutions that focus on vulnerabilities, configuration assessments, malware defenses, as well as activity and event monitoring.

References

[1] B. Harpham, Writer and Editor," How the Internet of Things is changing healthcare and transportation," CIO, 8 September 2015; http://www.cio.com/article/2981481/healthcare/how-the-internet-of-things-is-changing-healthcare-and-transportation.html

[2] J. Finkle, "J&J warns diabetic patients: Insulin pump vulnerable to hacking," TECHNOLOGY NEWS, 4 October, 2016; http://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L

[3] C. Brook, "Health and fitness applications poor at protecting privacy, FTC says," Threatpost, 8 May 2014; http://threatpost.com/health-and-fitness-applications-poor-at-protecting-privacy-ftc-says

[4] BCC Research, "Mobile health (mHealth) technologies and global markets 2014" 14 March 2014; http://www.bccresearch.com/market-research/healthcare/mobile-health-hlc162a.html

[5] Privacy Rights Clearinghouse. Fact Sheet 39: Mobile health and fitness applications: What are the privacy risks? (1 December 2014); https://www.privacyrights.org/mobile-health-and-fitness-applications-what-are-privacy-risks

[6] K. Michael, "Hackers create more IoT botnets with Mirai source code," PCWorld, 18 October 2016; http://www.pcworld.com/article/3132571/hackers-create-more-iot-botnets-with-mirai-source-code.html

[7] K. Lee, "Healthcare IoT security issues: Risks and what to do about them," December 2015; http://searchhealthit.techtarget.com/feature/Healthcare-IoT-security-issues-Risks-and-what-to-do-about-them

[8] C. Catalin, "Thousands of IoT Medical Devices Found Vulnerable to Online Attacks," 29 September 2015; http://news.softpedia.com/news/thousands-of-iot-medical-devices-found-vulnerable-to-online-attacks-493144.shtml

[9] T. William, "Healthcare's 'Internet of Things' should be the 'security of Things'," 19 May 2015; http://www.healthcareitnews.com/blog/healthcares-internet-things-should-be-security-things

[10] S. Mahmood, "Medjacking: The newest health care risk?" 24 September 2015; http://www.healthcareitnews.com/news/medjacking-newest-healthcare-risk

[11] T. Harriet, "How the 'Internet of Things' could be fatal," 4 March 2016; http://www.cnbc.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html

[12] Ayala Luis, "Cybersecurity for Hospitals and Healthcare facilities - A guide to detection and prevention" Fredericksburg, VA. www.allite.com